José Carlos Pol

TEORIA ELEMENTAR DOS NÚMEROS

Edgard de Alencar Filho

Ex-professor de GEOMETRIA ANALÍTICA e CÁLCULO da Escola Militar do Realengo e de MATEMÁTICA da Escola Preparatória de São Paulo

Juarez

CIP-Brasil. Catalogação-na-Fonte
Câmara Brasileira do Livro, SP

A353t Alencar Filho, Edgard de, 1913-
Teoria elementar dos números/Edgard de Alencar Filho. -- São Paulo : Nobel, 1981.

Bibliografia.
ISBN 85-213-0040-9

1. Números - Teoria I. Título.

17. CDD-512.31
18. -512.7

81-0333

Índices para catálogo sistemático:

1. Teoria dos números 512.31 (17.)
512.7 (18.)

ÍNDICE

CAPÍTULO 1 - NÚMEROS INTEIROS: NOÇÕES FUNDAMENTAIS

1.1 Números inteiros 13
1.2 Propriedades dos inteiros 14
1.3 Valor absoluto de um inteiro 16
1.4 Fatorial 18
1.5 Número binomial 20
1.6 Números binomiais complementares 21
1.7 Números binomiais consecutivos 21
Exercícios 25

CAPÍTULO 2 - INDUÇÃO MATEMÁTICA

2.1 Elemento mínimo de um conjunto de inteiros .. 31
2.2 Princípio da boa ordenação 32
2.3 Princípio de indução finita 34
2.4 Indução matemática 35
2.5 Exemplos de demonstração por indução matemática 37
2.6 Outras formas de indução matemática 40
Exercícios 45

CAPÍTULO 3 - SOMATÓRIOS E PRODUTÓRIOS

3.1 Somatórios 47
3.2 Propriedades dos somatórios 49
3.3 Somatórios duplos 50
3.4 Produtórios 52
3.5 Propriedades dos produtórios 53
3.6 Teorema do binômio 55
3.7 Triângulo de PASCAL 57
3.8 Propriedades do triângulo de PASCAL 59
3.9 Números triangulares 61
Exercícios 65

CAPÍTULO 4 - DIVISIBILIDADE

4.1 Relação de divisibilidade em Z 68
4.2 Conjunto dos divisores de um inteiro 71
4.3 Divisores comuns de dois inteiros 72
4.4 Algoritmo da divisão 74
4.5 Paridade de um inteiro 78
Exercícios 80

CAPÍTULO 5 - MÁXIMO DIVISOR COMUM

5.1 Máximo divisor comum de dois inteiros 84
5.2 Existência e unicidade do mdc 85
5.3 Inteiros primos entre si 89
5.4 Caracterização do mdc de dois inteiros 93
5.5 Mdc de vários inteiros 94
Exercícios 96

CAPÍTULO 6 - ALGORITMO DE EUCLIDES.
MÍNIMO MÚLTIPLO COMUM

6.1 Algoritmo de EUCLIDES 101
6.2 Múltiplos comuns de dois inteiros 108
6.3 Mínimo múltiplo comum de dois inteiros 110
6.4 Relação entre o mdc e o mmc 111
6.5 Mmc de vários inteiros 112
Exercícios 113

CAPÍTULO 7 - NÚMEROS PRIMOS

7.1 Números primos e compostos 116
7.2 Teorema fundamental da Aritmética 119
7.3 Fórmulas que dao primos 125
7.4 Crivo de ERATÓSTENES 126
7.5 Primos gêmeos 127
7.6 Sequências de inteiros consecutivos compostos128
7.7 Conjectura de GOLDBACH 129
7.8 Método de fatoração de FERMAT 131
Exercícios 132

CAPÍTULO 8 - EQUAÇÕES DIOFANTINAS LINEARES

8.1 Generalidades 137
8.2 Condição de existência de solução 138
8.3 Soluções da equação $ax + by = c$ 139
Exercícios 146

CAPÍTULO 9 - CONGRUÊNCIAS

9.1 Inteiros congruentes 148
9.2 Caracterização de inteiros congruentes 150
9.3 Propriedades das congruências 152
9.4 Sistemas completos de restos 159
Exercícios 162

CAPÍTULO 10 - CONGRUÊNCIAS LINEARES

10.1 Generalidades 165
10.2 Condição de existência de solução 167
10.3 Soluções da congruência $ax \equiv b \pmod{m}$ 168
10.4 Resolução de equações diofantinas lineares por congruências 175
10.5 Inverso de um inteiro 178
Exercícios 179

CAPÍTULO 11 - SISTEMAS DE CONGRUÊNCIAS LINEARES

11.1 Generalidades 181
11.2 Teorema do resto chinez 133
Exercícios 191

CAPÍTULO 12 - TEOREMAS DE FERMAT E WILSON

12.1 Teorema de FERMAT 193
12.2 Teorema de WILSON 199
Exercícios 203

CAPÍTULO 13 - DIVISORES DE UM INTEIRO

13.1 Divisores de um inteiro 205
13.2 Número de divisores 208
13.3 Soma de divisores 212
13.4 Notação 215
13.5 Produto de divisores 216
Exercícios 218

CAPÍTULO 14 - FUNÇÕES ARITMÉTICAS

14.1 Conceito de função aritmética 221
14.2 Funções aritméticas multiplicativas 222
14.3 Função de MOBIUS 227
14.4 Funções aritméticas multiplicativas completas 231
14.5 Função maior inteiro 231

14.6 Fórmula de inversão de MOBIUS 233
Exercícios 235

CAPÍTULO 15 - FUNÇÃO E TEOREMA DE EULER

15.1 Função de EULER 237
15.2 Cálculo de $\Phi(n)$ 240
15.3 Propriedades da função de EULER 244
15.4 Teorema de EULER 249
15.5 Relação entre as funções Φ e $\underline{u}$ 253
Exercícios 255

CAPÍTULO 16 - NÚMEROS PERFEITOS

16.1 Números perfeitos 258
16.2 Números multiperfeitos 265
16.3 Números amigos 266
16.4 Números deficientes e abundantes 267
16.5 Números de MERSENNE 268
16.6 Números de FERMAT 272
Exercícios 274

CAPÍTULO 17 - NÚMEROS DE FIBONACCI

17.1 Sequências recorrentes 278
17.2 Sequência de FIBONACCI 279
17.3 Somas de números de FIBONACCI 280
17.4 Soma dos quadrados de números de FIBONACCI.. 234
17.5 Identidades entre números de FIBONACCI 285
17.6 Propriedades dos números de FIBONACCI 287
Exercícios 292

CAPÍTULO 18 - TERNOS PITAGÓRICOS

18.1 Conceito de terno pitagórico 296
18.2 Fórmulas que dão ternos pitagóricos 297
18.3 Ternos pitagóricos primitivos 299
18.4 Propriedades dos ternos pitagóricos 301
Exercícios 305

CAPÍTULO 19 - CLASSES RESIDUAIS

19.1 Conceito de classe residual 308
19.2 Propriedades das classes residuais 310
19.3 Conjunto das classes residuais 312
Exercícios 317

CAPÍTULO 20 - REPRESENTAÇÃO DOS INTEIROS EM OUTRAS BASES. CRITÉRIOS DE DIVISIBILIDADE

20.1 Representação dos inteiros em outras bases.. 318
20.2 Critérios de divisibilidade 323
20.3 Critério de divisibilidade por 9 325
20.4 Critério de divisibilidade por 11 327
Exercícios 328

CAPÍTULO 21 - RAIZES PRIMITIVAS

21.1 Ordem de um inteiro módulo n 333
21.2 Raiz primitiva de um inteiro 341
Exercícios 344

EXERCÍCIOS SUPLEMENTARES 346

RESPOSTAS DOS EXERCÍCIOS 367

BIBLIOGRAFIA 385

PREFÁCIO

O conceito de número desempenha papel fundamental na civilização moderna, e as ciências mais avançadas são precisamente aquelas que mais empregam a linguagem dos números. Aliás, a Matemática vem se tornando cada vez mais necessária em todos os ramos do conhecimento humano, desde a Física à Biologia, bem como nas ciências sociais (Economia, Finanças, etc.). Até mesmo na Psicologia tem sido utilizada com êxito.

O livro que ora publicamos pela conceituada "Editora NOBEL" tem por única finalidade fornecer aos estudantes as primeiras noções da "Teoria dos Números". Desta forma procuro contribuir, na medida das minhas forças, para a melhoria do ensino da Matemática em nosso País, como, aliás, venho fazendo há muitos anos.

Em cada um dos Capítulos do livro os conceitos são definidos com precisão e as proposições fundamentais pertinentes são todas demonstradas e, logo em seguida, exemplificadas, tendo em vista o leitor que pela primeira vez aborda esta fascinante parte da Matemática pura. Além disso, cada Capítulo termina por um conjunto de Exercícios, numéricos e teóricos, cujas respostas são dadas no final do livro, os quais permitem completar a aprendizagem.

Edgard de Alencar Filho

CAPÍTULO 1

NÚMEROS INTEIROS NOÇÕES FUNDAMENTAIS

1.1 NÚMEROS INTEIROS

Os *números inteiros* ou apenas os *inteiros* são:

$$\ldots,-3,-2,-1,0,1,2,3,\ldots$$

cujo *conjunto* representa-se pela letra Z, isto é:

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

Neste conjunto Z destacam-se os seguintes *subconjuntos:*

(1) Conjunto Z* dos *inteiros não nulos* ($\neq 0$):

$$Z^* = \{ x \in Z \mid x \neq 0 \} = \{ \pm 1, \pm 2, \pm 3, \ldots \}$$

(2) Conjunto Z_+ dos *inteiros não negativos* ($\geqslant 0$):

$$Z_+ = \{ x \in Z \mid x \geqslant 0 \} = \{ 0,1,2,3, \ldots \}$$

(3) Conjunto Z_- dos *inteiros não positivos* ($\leqslant 0$):

$$Z_- = \{ x \in Z \mid x \leqslant 0 \} = \{0,-1,-2,-3, \ldots \}$$

(4) Conjunto Z_+^* dos *inteiros positivos* (> 0):

$$Z_+^* = \{x \in Z \mid x > 0\} = \{1, 2, 3, \ldots\}$$

(5) Conjunto Z_-^* dos *inteiros negativos* (< 0):

$$Z_-^* = \{x \in Z \mid x < 0\} = \{-1, -2, -3, \ldots\}$$

Os *inteiros positivos* são também denominados *inteiros naturais* e por isso o conjunto dos inteiros positivos é habitualmente designado pela letra $N (N = Z_+^*)$.

1.2 PROPRIEDADES DOS INTEIROS

O conjunto Z dos inteiros *munido* das operações de *adição* (+) e *multiplicação*(.) possui as propriedades fundamentais que a seguir enumeramos, onde a, b e c são inteiros quaisquer, isto é, elementos de Z:

(1) $a + b = b + a$ e $ab = ba$

(2) $(a + b) + c = a + (b + c)$ e $(ab)c = a(bc)$

(3) $0 + a = a$ e $1.a = a$

(4) $-a = (-1)a$ e $a - a = a + (-a) = 0$

(5) $a(b + c) = ab + ac$

(6) $0.a = 0$, e se $ab = 0$, então $a = 0$ ou $b = 0$.

Também existe uma *"relação de ordem"* entre os inteiros, representada pelo sinal "< (menor que)", que possui as seguintes propriedades:

(7) Se $a \neq 0$, então $a < 0$ ou $0 < a$

(8) Se $a < b$ e $b < c$, então $a < c$

(9) Se $a < b$, então $a + c < b + c$

(10) Se $a < b$ e $0 < c$, então $ac < bc$

(11) Se $a < b$ e $c < 0$, então $bc < ac$

Destas propriedades podem ser deduzidas muitas outras propriedades dos inteiros.

<u>Exemplo 1.1</u> Demonstrar: $-(a + b) = (-a) + (-b)$.

Com efeito, temos sucessivamente:

$-(a + b) = (-1)(a + b) =$ (Propriedade 4)

$= (-1)a + (-1)b =$ (Propriedade 5)

$= (-a) + (-b)$ (Propriedade 4)

<u>Exemplo 1.2</u> Demonstrar que, se $x \neq 0$, então $0 < x^2$.

Com efeito:

(1) Se $x \neq 0$, então $x < 0$ ou $0 < x$ (Propriedade 7)

(2) Se $x < 0$, então $0.x < x.x$ (Propriedade 11)

$0 < x^2$ (Propriedade 6)

(3) Se $0 < x$, então $0.x < x.x$ (Propriedade 10)

$0 < x^2$ (Propriedade 6)

N O T A - Com o mesmo significado de $a < b$, escreve-se $b > a$.

Indica-se, de modo abreviado, que $a < b$ ou $a = b$ por $a \leqslant b$. Por exemplo, temos $2 \leqslant 3$, porque $2 < 3$, e $2 \leqslant 2$, porque $2 = 2$.

Com o mesmo significado de $a \leqslant b$, escreve-se $b \geqslant a$.

Em lugar de $a \leqslant b$ e $b \leqslant c$ também se escreve $a \leqslant b \leqslant c$.

Análogos significados têm:

$$a \leqslant b < c, \quad a < b \leqslant c, \quad a > b \geqslant c, \quad \text{etc.}$$

1.3 VALOR ABSOLUTO DE UM INTEIRO

<u>Definição 1.1</u> Chama-se *valor absoluto* de um inteiro $\underline{a}$, o inteiro que se indica por $|a|$, e tal que

$$|a| = \begin{cases} a & \text{se} \quad a \geqslant 0 \\ -a & \text{se} \quad a < 0 \end{cases}$$

Assim, p.ex.:

$$|3| = 3 \quad \text{e} \quad |-5| = -(-5) = 5$$

Consoante a definição de $|a|$, para todo inteiro $\underline{a}$, temos:

$$|a| \geqslant 0, \quad |a|^2 = a^2, \quad |-a| = |a| \quad , \quad a \leqslant |a|$$

O *valor absoluto* $|a|$ de um inteiro $\underline{a}$ também pode ser definido pelas igualdades:

$$|a| = \sqrt{a^2}, \qquad |a| = \text{máx}(-a, a)$$

onde $\sqrt{a^2}$ denota a raiz quadrada *não negativa* de a^2 e máx(-a,a) indica o *maior* dos dois inteiros $-\underline{a}$ e $\underline{a}$.

Assim, p.ex.:

$$|-4| = \sqrt{(-4)^2} = \sqrt{16} = 4$$

$$|-6| = \text{máx}(-6,6) = 6$$

<u>Teorema 1.1</u> Se $\underline{a}$ e $\underline{b}$ são dois inteiros, então:

$$|ab| = |a| \cdot |b|$$

<u>Demonstração:</u>

Com efeito:

$$|ab| = \sqrt{(ab)^2} = \sqrt{a^2b^2} = \sqrt{a^2} \cdot \sqrt{b^2} = |a| \cdot |b|$$

<u>Teorema 1.2</u> Se $\underline{a}$ e $\underline{b}$ são dois inteiros, então:

$$|a + b| \leqslant |a| + |b|$$

<u>Demonstração:</u>

Com efeito, pela definição de $|a|$, temos:

$$-|a| \leqslant a \leqslant |a| \ , \quad -|b| \leqslant |b| \leqslant |b|$$

Somando ordenadamente estas desigualdades, obtemos:

$$-(|a| + |b|) \leqslant a + b \leqslant |a| + |b|$$

o que implica:

$$|a + b| \leqslant |a| + |b|$$

Corolário 1.1 Se a e b são dois inteiros, então:

$$|a - b| \leq |a| + |b|$$

Demonstração:

Com efeito:

$$|a - b| = |a + (-b)| \leq |a| + |-b| = |a| + |b|$$

1.4 FATORIAL

Definição 1.2 Chama-se *fatorial* de um inteiro *não negativo n* ($n \geq 0$), o inteiro que se indica por $n!$, e tal que:

$$n! = \begin{cases} 1 & \text{se } n = 0 \text{ ou } n = 1 \\ n(n-1)(n-2)\ldots 3.2.1 & \text{se } n \geq 2 \end{cases}$$

Assim, p.ex.:

$$7! = 7.6.5.4.3.2.1 = 5040$$

Observe-se que $n! = n.(n-1)!$.

Exemplo 1.3 Escrever, usando o *símbolo de fatorial*, o produto dos n primeiros inteiros positivos *pares* e o produto dos n primeiros inteiros positivos *ímpares*.

Os n primeiros inteiros positivos *pares* são:

$$2, 4, 6, \ldots, 2n-2, 2n$$

isto é:

$$2.1, 2.2, 2.3, \ldots, 2.(n-1), 2.n$$

Portanto:

$$2.4.6...(2n-2).2n = 2^n(1.2.3...(n-1).n) = 2^n.n!$$

Os n primeiros inteiros positivos *ímpares* são:

$$1,\ 3,\ 5,\ ...,\ 2n-3,\ 2n-1$$

Portanto:

$$1.3.5...(2n-3).(2n-1) = \frac{1.2.3.4...(2n-2).(2n-1).2n}{2.4.6...(2n-2).2n}$$

$$= \frac{(2n)!}{2^n.n!}$$

Exemplo 1.4 Calcular a soma:

$$1.1! + 2.2! + 3.3! + ... + n.n!$$

Tomemos a igualdade:

$$k.k! = (k + 1)! - k!$$

e nela façamos sucessivamente $k = 1,2,3,...,n$, o que dá:

$$1.1! = 2! - 1$$

$$2.2! = 3! - 2!$$

$$3.3! = 4! - 3!$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$n.n! = (n + 1)! - n!$$

Somando ordenadamente todas essas n igualdades e simplificando, obtemos:

$$1.1! + 2.2! + 3.3! + \ldots + n.n! = (n + 1)! - 1$$

1.5 NÚMERO BINOMIAL

Definição 1.3 Sejam $n > 0$ e k dois inteiros tais que

$$0 \leqslant k \leqslant n.$$

Chama-se *número binomial de numerador* n e *classe k*, o inteiro que se indica por $\binom{n}{k}$, e tal que

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

Obviamente, também podemos escrever:

$$\binom{n}{k} = \frac{n(n-1)\ldots(k+1)}{(n-k)!} = \frac{n(n-1)\ldots(n-k+1)}{k!}$$

Em particular, para $k = 0$ ou $k = n$, temos:

$$\binom{n}{0} = \binom{n}{n} = 1$$

Assim, p.ex.:

$$\binom{8}{3} = \frac{8!}{3!5!} = \frac{3.7.6.5.4.3.2.1}{3.2.1.5.4.3.2.1} = \frac{8.7.6}{3.2.1} = 56$$

$$\binom{7}{4} = \frac{7.6.5}{(7-4)!} = \frac{7.6.5}{3.2.1} = 35$$

1.6 NÚMEROS BINOMIAIS COMPLEMENTARES

Definição 1.4 Chamam-se *números binomiais complementares* dois números binomiais que têm o mesmo numerador e cuja soma das suas classes respectivas é igual ao numerador comum.

Assim, p.ex.; $\binom{20}{7}$ e $\binom{20}{13}$ são *números binomiais complementares*, pois, têm o mesmo numerador 20 e 7 + 13 = 20.

Teorema 1.3 Dois números binomiais complementares são iguais.

Demonstração:

Sejam $\binom{n}{k}$ e $\binom{n}{h}$ dois números binomiais complementares. Então, $k + h = n$ e $k = n - h$. Portanto:

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

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

1.7 NÚMEROS BINOMIAIS CONSECUTIVOS

Definição 1.5 Chamam-se *números binomiais consecutivos* dois números binomiais que têm o mesmo numerador e cujas classes respectivas são inteiros consecutivos.

Assim, p.ex., $\binom{18}{9}$ e $\binom{18}{10}$ são *números binomiais consecu-*

tivos, pois, têm o mesmo numerador 18 e as suas classes respectivas são os inteiros consecutivos 9 e 10.

Teorema 1.4 Entre dois números binomiais consecutivos $\binom{n}{k-1}$ e $\binom{n}{k}$, com $1 \leqslant k \leqslant n$, subsiste a *relação de STIFEL:*

$$\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$$

Demonstração:

Com efeito:

$$\binom{n}{k-1} + \binom{n}{k} = \frac{n!}{(k-1)!(n-k+1)!} + \frac{n!}{k!(n-k)!} =$$

$$= \frac{n!}{(k-1)!(n-k+1)(n-k)!} + \frac{n!}{k(k-1)!(n-k)!} =$$

$$= \frac{n!}{(k-1)!(n-k)!}\left(\frac{1}{n-k+1} + \frac{1}{k}\right) =$$

$$= \frac{n!}{(k-1)!(n-k)!} \cdot \frac{n+1}{k(n-k+1)} =$$

$$= \frac{(n+1)!}{k!(n+1-k)!} = \binom{n+1}{k}$$

Assim, p.ex.:

$$\binom{18}{9} + \binom{18}{10} = \binom{19}{10}$$

$$\binom{13}{8} = \binom{12}{8} + \binom{12}{7}$$

<u>Corolário 1.2</u> $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-2}{k-1} + \ldots + \binom{k}{k-1} + \binom{k-1}{k-1}$

<u>Demonstração:</u>

Com efeito, mudando na relação de STIFEL <u>n</u> sucessivamente por n-1, n-2, n-3, ..., k, obtemos:

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

$$\binom{n-1}{k} = \binom{n-2}{k-1} + \binom{n-2}{k}$$

$$\binom{n-2}{k} = \binom{n-3}{k-1} + \binom{n-3}{k}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\binom{n+1}{k} = \binom{k}{k-1} + \binom{k}{k}$$

Além disso, é evidente: $\binom{k}{k} = \binom{k-1}{k-1}$.

Somando ordenadamente todas essas igualdades e suprimindo os termos comuns aos dois membros acha-se a relação desejada.

Substituindo, nesta relação, cada número binomial pelo seu *complementar*, obtemos:

$$\binom{n}{n-k} = \binom{n-1}{n-k} + \binom{n-2}{n-k-1} + \ldots + \binom{k}{1} + \binom{k-1}{0}$$

<u>Corolário 1.3</u> $\binom{n}{k} = \binom{n-1}{k} + \binom{n-2}{k-1} + \ldots + \binom{n-k}{1} + \binom{n-k-1}{0}$

Demonstração:

Consoante a *relação de STIFEL*, temos:

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

$$\binom{n-1}{k-1} = \binom{n-2}{k-2} + \binom{n-2}{k-1}$$

$$\binom{n-2}{k-2} = \binom{n-3}{k-3} + \binom{n-3}{k-2}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\binom{n-k+1}{1} = \binom{n-k}{0} + \binom{n-k}{1}$$

Além disso, temos:

$$\binom{n-k}{0} = \binom{n-k-1}{0}$$

Somando ordenadamente todas essas igualdades e suprimindo os termos comuns aos dois membros acha-se a relação desejada.

EXERCÍCIOS

1. Calcular a soma dos n primeiros inteiros positivos.
2. Calcular o inteiro positivo n sabendo:

$$3^{n+2} . 2^{n+3} = 2592$$

3. Calcular o inteiro positivo n sabendo:

$$3^n + 3^{n+1} + 3^{n+2} + 3^{n+3} = 1080$$

4. Achar os valores de $n \leqslant 7$ para os quais $n! + 1$ é um *quadrado perfeito*.

5. Sendo m e n inteiros positivos, dizer se é *verdadeiro* ou *falso:*

$$(mn)! = m!n! \quad e \quad (m+n)! = m' + n!$$

6. Demonstrar:

$$(n-1)! \left[(n+1)! - n!\right] = (n!)^2$$

7. Sendo $n \geqslant 2$, demonstrar: $(n^2)! > (n!)^2$.

8. Decompor o inteiro 565 numa soma de cinco inteiros ímpares consecutivos.

9. Achar todas as soluções inteiras e positivas da equação:

$$(x + 1)(y + 2) = 2xy$$

10. Achar um inteiro positivo de dois algarismos que seja igual ao quádruplo da soma dos seus algarismos.

11. Achar o menor e o maior inteiro positivo de n algarismos.

12. Resolver a equação: $(x + 2)! = 72.x!$.

13. Resolver a equação:

$$\binom{7}{x^2-x} = \binom{7}{2x-2}$$

14. Demonstrar:

$$\binom{n}{k} = \frac{n-k+1}{k}\binom{n}{k-1}$$

15. Achar todas as soluções inteiras e positivas da equação:

$$x^2 - y^2 = 88$$

16. Verificar que o quadrado de um inteiro não pode terminar em 2, 3, 7 ou 8.

17. Reconstituir as adições:

(a) $3 * 76 + 2 * * * + 5 * 28 = 12838$

(b) $5 * 23 + 40 * * + 1269 = 1 * 927$

18. Reconstituir as subtrações:

(a) $1 * 256 - 431 * = 89 * 6$

(b) $63 * 1 - 43 * = 5 * 86$

19. O produto de um inteiro positivo de três algarismos por 7 termina à direita por 638. Achar esse inteiro.

20. Determinar quantos algarismos se empregam para numerar todas as páginas de um livro que tem 2748 páginas.

21. Reconstituir as multiplicações:

(a)

```
    4 3 5
      * 6
  -------
  * 6 * 0
1 3 0 5
-------
1 * 6 6 0
```

(b)

```
    2 * 0 3
        * 2
  -------
    4 8 0 6
1 4 * 1 *
---------
1 4 8 9 8 6
```

22. Calcular a soma dos três *maiores* inteiros de, respectivamente, três, quatro e cinco algarismos.

23. Determinar a diferença entre o maior inteiro com seis algarismos diferentes e o maior inteiro com cinco algarismos também diferentes.

24. Um livro tem 1235 páginas. Determinar o número de vezes que o algarismo 1 aparece na numeração das páginas deste livro.

25. Reconstituir as divisões:

(a)
```
* * 8 * | * *
        |-------
  * 9 1 |  3 2
    4 * |
```

(b)
```
* 6 * 1 | * * *
       |-------
     5 9 |  6
```

26. Mostrar que o produto de quatro inteiros consecutivos, aumentado de 1, é um quadrado perfeito.

27. A soma dos quadrados de dois inteiros é 3332 e um deles é o quádruplo do outro. Achar os dois inteiros.

28. Sejam a e b dois inteiros. Demonstrar:

$$\text{máx}(a,b) = (a + b + |a - b|)/2$$
$$\text{mín}(a,b) = (a + b - |a - b|)/2$$

29. Determinar o inteiro $n > 1$ de modo que a soma

$$1! + 2! + 3! + \ldots + n!$$

seja um quadrado perfeito.

30. A média aritmética de dois inteiros positivos é 5 e a média geométrica é 4. Achar os dois inteiros.

31. Achar os cinco inteiros positivos consecutivos cuja soma dos quadrados é igual a 2010.

32. O *resto por falta* da raiz quadrada de um inteiro positivo é 135 e o *resto por excesso* é 38. Achar esse inteiro.

33. Resolver a equação: $\dfrac{x! + 3(x-2)!}{x! - 3(x-2)!} = \dfrac{31}{29}$

34. Achar o inteiro que deve ser somado a cada um dos inteiros 2, 6 e 14 para que, nesta ordem, formem uma *proporção contínua*.

35. Mostrar que o produto 12345679 x 9 x k, sendo $k \neq 0$ um algarismo, é kkk.kkk.kkk.

36. Achar o valor mínimo de uma soma de 10 inteiros positivos distintos, cada um dos quais se escreve com três algarismos.

37. Mostrar que o produto 37037037 x 3 x k, sendo $k \neq 0$ um algarismo, é kkk.kkk.kkk.

38. Um estudante ao efetuar a multiplicação de 7432 por um certo inteiro achou o produto 1731656, tendo trocado, por engano, o algarismo das dezenas do multiplicador, tomando um 3 em vez de 8. Achar o verdadeiro produto.

39. Achar o menor inteiro cujo produto por 21 é um inteiro formado apenas com algarismos 4.

40. Escreve-se a sequência natural dos inteiros positivos, sem separar os algarismos:

123456789101112131415...

Determinar:

(a) o 435º algarismo que se escreve;

(b) o 1756º algarismo que se escreve;

(c) o 12387º algarismo que se escreve.

41. Escreve-se a sequência natural dos inteiros positivos pares, sem separar os algarismos:

24681012141618...

Determinar o 2574º algarismo que se escreve.

42. Reconstituir as multiplicações:

(a)
```
    * * * *
      * *
  -------
  * * * * *
  * * * *
  -------
  9 0 3 2 9
```

(b)
```
      * * *
      * * *
  -------
    * * * *
  * * *
  -------
  3 6 7 3 3
```

43. Mostrar que o produto de dois fatores *entre* 10 e 20 é o décuplo da soma do primeiro com as unidades do segundo, mais o produto das unidades dos dois.

44. Achar o menor inteiro positivo que multiplicado por 33 dá um produto cujos algarismos são todos 7.

45. Os inteiros $\underline{a}$ e $\underline{b}$ são tais que $4 < a < 7$ e $3 < b < 4$. Mostrar que $0 < a - b < 4$.

46. Os inteiros $\underline{a}$ e $\underline{b}$ são tais que $-1 < a < 3$ e $-2 \leqslant b \leqslant 0$. Mostrar que $-1 < a - b < 5$.

47. Os inteiros $\underline{a}$ e $\underline{b}$ são tais que $-2 \leqslant a \leqslant 2$ e $-2 \leqslant b \leqslant 2$. Mostrar que $-4 \leqslant a - b \leqslant 4$.

CAPÍTULO 2

INDUÇÃO MATEMÁTICA

2.1 ELEMENTO MÍNIMO DE UM CONJUNTO DE INTEIROS

Definição 2.1 Seja A um conjunto de inteiros. Chama-se *elemento mínimo de* A um elemento $a \in A$ tal que $a \leqslant x$ para todo $x \in A$.

Representa-se pela notação "minA", que se lê: "mínimo de A". Portanto, simbolicamente:

$$\min A = a \Longleftrightarrow (a \in A \quad e \quad (\forall x \in A)\ (a \leqslant x))$$

Teorema 2.1 Se a é *elemento mínimo de* A, então este elemento é *único*.

Demonstração:

Com efeito, se existisse um outro *elemento mínimo* b *de* A, teríamos:

(i) $a \leqslant b$, porque $a = \min A$

(ii) $b \leqslant a$, porque $b = \min A$

Logo, pela propriedade *anti-simétrica* da relação de ordem natural "$\leqslant$" em Z, temos $a = b$.

O *elemento mínimo* de A, se existe, denomina-se também *primeiro elemento de* A ou *menor elemento de* A.

Exemplo 2.1 O conjunto $N = \{1,2,3,\ldots\}$ dos *inteiros positivos* tem o *elemento mínimo*, que é 1 ($\min N = 1$), porque $1 \in N$ e $1 \leqslant n$ para todo $n \in N$.

Exemplo 2.2 O conjunto $A = \{x \in Z \mid x > 12\}$ tem o *elemento mínimo*, que é 13 ($\min A = 13$), porque $13 \in A$ e $13 \leqslant x$ para todo $x \in A$.

Exemplo 2.3 O conjunto $Z_- = \{0,-1,-2,-3,\ldots\}$ dos *inteiros não positivos não tem o elemento mínimo*, porque não existe $a \in Z_-$ tal que $a \leqslant x$ para todo $x \in Z_-$.

Exemplo 2.4 O conjunto $A = \{x \in N \mid 3 \text{ divide } x^2\}$ tem o *elemento mínimo* 3 ($\min A = 3$), porque $3 \in A$ (3 divide 9) e $3 \leqslant x$ para todo $x \in A$ ($1 \notin A$ e $2 \notin A$).

2.2 PRINCÍPIO DA BOA ORDENAÇÃO

Todo conjunto não vazio A *de inteiros não negativos possui o elemento mínimo.*

Em outros termos, todo *subconjunto* não vazio A do conjunto

$$Z_+ = \{0,1,2,3,\ldots\}$$

dos *inteiros não negativos* $(\phi \neq A \subset Z_+)$ possui o *elemento mínimo*, isto é, simbolicamente:

$$(\forall A \subset Z_+,\ A \neq \phi) \Longrightarrow \exists\ \min A$$

Exemplo 2.5 O conjunto $A = \{1,3,5,7,\ldots\}$ dos *inteiros positivos ímpares* é um *subconjunto* não vazio de

$$Z_+ \ (\phi \neq A \subset Z_+).$$

Logo, pelo *"Princípio da boa ordenação"*, A possui o *elemento mínimo* $(\min A = 1)$.

Exemplo 2.6 O conjunto $P = \{2,3,5,7,11,\ldots\}$ dos *inteiros primos* é um *subconjunto* não vazio de $Z_+ (\phi \neq P \subset Z_+)$. Logo, pelo *"Princípio da boa ordenação"*, P possui o *elemento mínimo* $(\min P = 2)$.

Teorema 2.2 (de ARCHIMEDES) Se a e b são dois inteiros positivos quaisquer, então existe um inteiro positivo n tal que $na \geq b$.

Demonstração:

Suponhamos que a e b são dois inteiros positivos para os quais $na < b$ para todo inteiro positivo n. Então, todos os elementos do conjunto:

$$S = \{ b - na \mid n \in N \}$$

são *inteiros positivos* e, pelo *"Princípio da boa ordenação"*, S possui o *elemento mínimo*, digamos $\min S = b-ka$.

E como $b - (k + 1)a$ pertence a S, porque S contém todos os inteiros positivos desta forma, temos:

$$b - (k+1)a = (b - ka) - a < b - ka$$

isto é, $b - ka$ não é o *elemento mínimo de* S, o que é uma *contradição*. Logo, a *propriedade archimediana* é verdadeira.

Assim, p.ex.:

(i) se $a = 2$ e $b = 11$, então $n = 6$, porque $6.2 > 11$;
(ii) se $a = 9$ e $b = 5$, então $n = 1$, porque $1.9 > 5$.

2.3 PRINCÍPIO DE INDUÇÃO FINITA

<u>Teorema 2.3</u> Seja S um *subconjunto* do conjunto N dos inteiros positivos ($S \subset N$) que satisfaz as duas seguintes condições:

(1) 1 pertence a S ($1 \in S$);
(2) para todo inteiro, positivo <u>k</u>, se $k \in S$, então $k + 1 \in S$.

Nestas condições, S é o conjunto N dos inteiros positivos: $S = N$.

<u>Demonstração:</u>

Suponhamos, por absurdo, que S não é o conjunto N dos inteiros positivos ($S \neq N$) e seja X o conjunto de todos os

inteiros positivos que não pertencem a S, isto é:

$$X = \{x \mid x \in N \text{ e } x \notin S\} = N - S$$

Então, X é um *subconjunto* não vazio de $N(\phi \neq X \subset N)$ e, pelo "*Princípio da boa ordenação*", existe o *elemento mínimo* x_o de $X(\min X = x_o)$.

Pela condição (1), $1 \in S$, de modo que $x_o > 1$ e, portanto, $x_o - 1$ é um inteiro positivo que não pertence a X. Logo, $x_o - 1 \in S$ e, pela condição (2), segue-se que $(x_o - 1) + 1 = x_o \in S$, o que é uma *contradição*, pois, $x_o \in X = N - S$, isto é, $x_o \notin S$. Assim sendo, $X = \phi$ e $S = N$.

Consoante este "*Princípio de indução finita*", o único *subconjunto* de N que satisfaz às condições (1) e (2) é o próprio N.

2.4 INDUÇÃO MATEMÁTICA

<u>Teorema 2.4</u> Seja P(n) uma proposição associada a cada inteiro positivo <u>n</u> e que satisfaz às duas seguintes condições:

(1) P(1) é verdadeira;

(2) para todo inteiro positivo <u>k</u>, se P(k) é verdadeira, então P(k+1) também é verdadeira.

Nestas condições, a proposição P(n) é verdadeira para todo inteiro positivo <u>n</u>.

Demonstração:

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

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

Pela condição (1), P(1) é verdadeira e, portanto, $1 \in S$. Pela condição (2), para todo inteiro positivo k, se $k \in S$, então $k+1 \in S$. Logo, o conjunto S satisfaz às condições (1) e (2) do *"Princípio de indução finita"* e, portanto, S=N, isto é, a proposição P(N) é verdadeira para todo inteiro positivo n.

NOTA. O teorema 2.4 é geralmente denominado *"Teorema da indução matemática"* ou *"Princípio de indução matemática"*, e a demonstração de uma proposição usando-se este teorema chama-se *"demonstração por indução matemática"* ou *"demonstração por indução sobre n"*.

Na *"demonstração por indução matemática"* de uma dada proposição P(n) é *obrigatório verificar* que as condições (1) e (2) são ambas satisfeitas. A verificação da condição(1) é geralmente muito fácil, mas a verificação da condição (2) implica em demonstrar o *teorema auxiliar* cuja *hipótese* é:

H: proposição P(k) é verdadeira, $k \in N$

denominada *"hipótese de indução"*, e cuja *tese* ou *conclusão* é:

T: proposição P(k+1) é verdadeira.

2.5 EXEMPLOS DE DEMONSTRAÇÃO POR INDUÇÃO MATEMÁTICA

Exemplo 2.7 Demonstrar a proposição:

$$P(n) : 1 + 3 + 5 + \ldots + (2n - 1) = n^2, \quad \forall\, n \in N$$

Demonstração:

(1) P(1) é verdadeira, visto que $1 = 1^2$.

(2) A *hipótese de indução* é que a proposição:

$$P(k): 1 + 3 + 5 + \ldots + (2k - 1) = k^2, \qquad k \in N$$

é verdadeira.

Adicionando 2k+1 a ambos os membros desta igualdade, obtemos:

$$1 + 3 + 5 + \ldots + (2k-1) + (2k+1) =$$
$$= k^2 + (2k+1) = (k+1)^2$$

e isto significa que a proposição P(k+1) é verdadeira. Logo, pelo *"Teorema da indução matemática"*, a proposição P(n) é verdadeira para todo inteiro positivo n.

Exemplo 2.8 Demonstrar a proposição:

$$P(n) : \frac{1}{1.2} + \frac{1}{2.3} + \frac{1}{3.4} + \ldots + \frac{1}{n(n+1)} = \frac{n}{n+1}, \quad \forall\, n \in N$$

Demonstração:

(1) P(1) é verdadeira, visto que $\frac{1}{1.2} = \frac{1}{1+1}$.

(2) A *hipótese de indução* é que a proposição:

$$P(k): \frac{1}{1.2} + \frac{1}{2.3} + \frac{1}{3.4} + \ldots + \frac{1}{k(k+1)} = \frac{k}{k+1}, \qquad k \in N$$

é verdadeira.

Adicionando $\frac{1}{(k+1)(k+2)}$ a ambos os membros desta igualdade, obtemos:

$$\frac{1}{1.2} + \frac{1}{2.3} + \frac{1}{3.4} + \ldots + \frac{1}{k(k+1)} + \frac{1}{(k+1)(k+2)} =$$

$$= \frac{k}{k+1} + \frac{1}{(k+1)(k+2)} = \frac{k^2+2k+1}{(k+1)(k+2)} = \frac{k+1}{k+2}$$

e isto significa que a proposição $P(k+1)$ é verdadeira. Logo, pelo *"Teorema da indução matemática"*, a proposição $P(n)$ é verdadeira para todo inteiro positivo n.

Exemplo 2.9 Demonstrar a proposição:

$$P(n) : 3 \mid (2^{2n} - 1), \quad \forall\ n \in N$$

Demonstração:

(1) $P(1)$ é verdadeira, visto que $3 \mid (2^2 - 1)$.

(2) A *hipótese de indução* é que a proposição:

$$P(k) : 3 \mid (2^{2k} - 1), \qquad k \in N$$

é verdadeira. Portanto:

$$2^{2k} - 1 = 3q, \text{ com } q \in Z$$

o que implica:

$$2^{2(k+1)} - 1 = 2^2.2^{2k} - 1 = 4.2^{2k} - 1 =$$

$$= 4.2^{2k} - 4 + 4 - 1 = 4(2^{2k} - 1) + 3 =$$

$$= 4.3q + 3 = 3(4q + 1)$$

isto é, a proposição P(k+1) é verdadeira. Logo, pelo *"Teorema da indução matemática"*, a proposição P(n) é verdadeira para todo inteiro positivo n.

Exemplo 2.10 Demonstrar a proposição:

$$P(n): \quad 2^n > n, \qquad \forall\, n \in N$$

Demonstração:

(1) P(1) é verdadeira, visto que $2^1 = 2 > 1$.

(2) A *hipótese de indução* é que a proposição:

$$P(k): \quad 2^k > k, \qquad k \in N$$

é verdadeira. Portanto:

$$2.2^k > 2k \quad \text{ou} \quad 2^{k+1} > k + k \geq k + 1$$

o que implica: $2^{k+1} > k + 1$, isto é, a proposição P(k+1) é verdadeira. Logo, pelo *"Teorema da indução matemática"*, a proposição P(n) é verdadeira para todo inteiro positivo n.

2.6 OUTRAS FORMAS DA INDUÇÃO MATEMÁTICA

Teorema 2.5 Seja r um inteiro positivo fixo e seja $P(n)$ uma proposição associada a cada inteiro $n \geq r$ e que satisfaz às duas seguintes condições:

(1) $P(r)$ é verdadeira;

(2) para todo inteiro $k \geq r$, se $P(k)$ é verdadeira, então $P(k+1)$ também é verdadeira.

Nestas condições, $P(n)$ é verdadeira para todo inteiro $n \geq r$.

Demonstração:

Seja S o conjunto de todos os inteiros positivos n para os quais a proposição $P(r + n - 1)$ é verdadeira, isto é:

$$S = \{ n \in N \mid P(r + n - 1) \text{ é verdadeira } \}$$

Pela condição (1), $P(r) = P(r + 1 - 1)$ é verdadeira, isto é, $1 \in S$. E, pela condição (2), se $P(r + k - 1)$ é verdadeira, então:

$$P((r + k - 1) + 1) = P(r + (k + 1) - 1)$$

também é verdadeira, isto é, se $k \in S$, então $k+1 \in S$. Logo, pelo "*Princípio de indução finita*", S é o conjunto dos inteiros positivos: $S = N$, isto é, a proposição $P(r + n - 1)$ é verdadeira para todo $n \in N$, ou seja, o que é a mesma coisa, a proposição $P(n)$ é verdadeira para todo inteiro $n \geq r$.

Exemplo 2.11 Demonstrar a proposição:

$$P(n) : \quad 2^n < n! \ , \qquad \forall \ n \geq 4$$

Demonstração:

(1) P(4) é verdadeira, visto que $2^4 = 16 < 4! = 24$.

(2) Suponhamos, agora, que é verdadeira a proposição:

$$P(k) : \quad 2^k < k! \ , \qquad k \geq 4$$

Então, por ser $2 < k+1$ para $k \geq 4$, temos:

$$2^{k+1} < k! \ . \ (k+1) \quad \text{ou} \quad 2^{k+1} < (k+1)!$$

isto é, a proposição P(k+1) é verdadeira. Logo, pelo teorema 2.5, a proposição P(n) é verdadeira para todo inteiro $n \geq 4$.

Observe-se que a proposição P(n) é *falsa* para n = 1,2,3, pois, temos:

$$2^1 > 1! \ , \quad 2^2 > 2! \ , \quad 2^3 > 3!$$

Exemplo 2.12 Demonstrar a proposição:

$$P(n) : \quad n^2 > 2n+1 \ , \qquad \forall \ n \geq 3$$

Demonstração:

(1) P(3) é verdadeira, visto que $3^2 = 9 > 2.3 + 1 = 7$.

(2) Suponhamos, agora, que é verdadeira a proposição:

$$P(k) \ : \ k^2 > 2k+1 \ , \qquad k \geq 3$$

Então, temos:

$$k^2 + (2k+1) > (2k+1) + (2k+1)$$

$$(k+1)^2 > 2(k+1) + 2k \geq 2(k+1) + 6$$

e, portanto:

$$(k+1)^2 > 2(k+1) + 1$$

isto é, a proposição $P(k+1)$ é verdadeira. Logo, pelo teorema 2.5, a proposição $P(n)$ é verdadeira para todo inteiro $n \geq 3$.

Observe-se que a proposição $P(n)$ é *falsa* para $n = 1$ e $n = 2$, pois, temos:

$$1^2 < 2.1 + 1 \quad \text{e} \quad 2^2 < 2.2 + 1$$

<u>Teorema 2.6</u> Seja $P(n)$ uma proposição associada a cada inteiro positivo <u>n</u> e que satisfaz às duas seguintes condições:

(1) $P(1)$ é verdadeira;

(2) para todo inteiro positivo <u>k</u>, se

$$P(1), P(2), \ldots, P(k)$$

são todas verdadeiras, então $P(k+1)$ também é verdadeira.

Nestas condições, a proposição P(n) é verdadeira para todo inteiro positivo n.

Demonstração:

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

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

Suponhamos, por absurdo, que $S \neq N$ e seja X o conjunto de todos os inteiros positivos que não pertencem a S, isto é:

$$X = \{ x \mid x \in N \text{ e } x \notin S \} = N - S$$

Então, X é um *subconjunto* não vazio de N e, pelo *"Princípio da boa ordenação"*, existe o *elemento mínimo* j de X (minX = j).

Pela condição (1), $1 \in S$, de modo que $j > 1$, e como j é o menor inteiro positivo que não pertence a S, segue-se que as proposições P(1), P(2),...,P(j-1) são todas verdadeiras. Então, pela condição (2), a proposição P(j) é verdadeira e $j \in S$, o que é uma *contradição*, pois, $j \in X$, isto é, $j \notin S$. Assim sendo, $S = N$ e a proposição P(n) é verdadeira para todo inteiro positivo n.

Teorema 2.7 Seja r um inteiro positivo fixo e seja P(n) uma proposição associada a cada inteiro $n \geq r$ e que satisfaz às duas seguintes condições:

(1) $P(r)$ é verdadeira;

(2) para todo inteiro $k > r$, se $P(m)$ é verdadeira para todo inteiro $\underline{m}$ tal que $r \leqslant m < k$, então $P(k)$ é verdadeira.

Nestas condições, a proposição $P(n)$ é verdadeira para todo inteiro $n \geqslant r$.

Demonstração:

Seja S o conjunto de todos os inteiros $n \geqslant r$ para os quais a proposição $P(n)$ é *falsa*, isto é:

$$S = \{ n \in N \mid n \geqslant r \text{ e } P(n) \text{ é falsa} \}$$

Suponhamos, por absurdo, que S não é vazio ($S \neq \phi$). Então, pelo *"Princípio da boa ordenação"*, existe o *elemento mínimo* $\underline{j}$ de S ($\min S = j$).

Pela condição (1), $r \notin S$, de modo que $j > r$, e por conseguinte $P(m)$ é verdadeira para todo inteiro $\underline{m}$ tal que $r \leqslant m < j$. Assim sendo, pela condição (2), $P(j)$ é verdadeira e $j \notin S$, o que é uma *contradição*, pois, $j \in S$. Logo, o conjunto S é vazio ($S = \phi$), e a proposição $P(n)$ é verdadeira para todo inteiro $n \geqslant r$.

EXERCÍCIOS

1. Demonstrar por "indução matemática":

(a) $1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n}{6}(n+1)(2n+1), \quad \forall\, n \in N$

(b) $1^3 + 2^3 + 3^3 + \ldots + n^3 = \frac{n^2}{4}(n+1)^2, \quad \forall\, n \in N$

(c) $1^2 + 3^2 + 5^2 + \ldots + (2n-1)^2 = \frac{n}{3}(4n^2-1), \quad \forall\, n \in N$

(d) $1^3 + 3^3 + 5^3 + \ldots + (2n-1)^3 = n^2(2n^2-1), \quad \forall\, n \in N$

(e) $1.2 + 2.3 + 3.4 + \ldots + n(n+1) = \frac{n}{3}(n+1)(n+2), \forall\, n \in N$

(f) $1 + \frac{1}{4} + \frac{1}{9} + \ldots + \frac{1}{n^2} \leqslant 2 - \frac{1}{n}, \quad \forall\, n \in N$

(g) $a + aq + aq^2 + \ldots + aq^n = \frac{a(q^{n+1}-1)}{q-1} \; (q \neq 1), \quad \forall\, n \in N$

2. Demonstrar por "indução matemática":

(a) $2^n < 2^{n+1}, \quad \forall\, n \in N$ (b) $2^n > n^2, \quad \forall\, n \geqslant 5$

(c) $2^n > n^3, \quad \forall\, n \geqslant 10$ (d) $4^n > n^4, \quad \forall\, n \geqslant 5$

(e) $n! > n^2, \quad \forall\, n \geqslant 4$ (f) $n! > n^3, \quad \forall\, n \geqslant 6$

3. Demonstrar por "indução matemática":

(a) $2 \mid (3^n-1), \quad \forall\, n \in N$

(b) $6 \mid (n^3 - n), \quad \forall\, n \in N$

(c) $5 \mid (3^n - 3^n), \quad \forall\, n \in N$

(d) $24 \mid (5^{2n} - 1), \quad \forall\, n \in N$

(e) $7 \mid (2^{3n} - 1), \quad \forall\, n \in N$

(f) $8 \mid (3^{2n} + 7), \quad \forall\, n \in N$

4. Demonstrar que $10^{n+1} - 9n - 10$ é um *múltiplo* de 81 para todo inteiro positivo n.

5. Demonstrar que $\frac{n^3}{3} + \frac{n^5}{5} + \frac{7n}{15}$ é um inteiro positivo para todo $n \in N$.

CAPÍTULO 3

SOMATÓRIOS E PRODUTÓRIOS

3.1 SOMATÓRIOS

Sejam os $n > 1$ inteiros $a_1, a_2, \ldots, a_n$. Para indicar, de modo abreviado, a *soma* $a_1 + a_2 + \ldots + a_n$ desses n inteiros usa-se a notação:

$$\sum_{i=1}^{n} a_i$$

que se lê: "somatorio de a_i de 1 a n".

Em particular, para $n = 2, 3, \ldots,$ temos:

$$\sum_{i=1}^{2} a_i = a_1 + a_2, \qquad \sum_{i=1}^{3} a_i = a_1 + a_2 + a_3, \ldots$$

A letra i chama-se o *índice do somatório* e pode ser substituida por qualquer outra diferente de a e de n - é um *índice mudo*. E os inteiros 1 e n que figuram abaixo e acima da letra grega maiúscula Σ (sigma) chamam-se respectivamente *limite inferior* e *limite superior* do índice i.

O número de *parcelas* de um somatório é sempre igual à diferença entre os limites superior e inferior do seu índice mais uma unidade.

Se m e n são dois inteiros, com $m \leq n$, então, por definição:

$$\sum_{i=m}^{n} a_i = a_m + a_{m+1} + a_{m+2} + \ldots + a_n$$

Exemplo 3.1 Temos:

$$\sum_{i=1}^{7} 5i = 5.1 + 5.2 + 5.3 + 5.4 + 5.5 + 5.6 + 5.7 =$$

$$= 5 + 10 + 15 + 20 + 25 + 30 + 35 = 140$$

$$\sum_{j=1}^{4} (8j-3) = (8.1-3) + (8.2-3) + (8.3-3) + (8.4-3) =$$

$$= 5 + 13 + 21 + 29 = 68$$

$$\sum_{k=3}^{8} k.2^k = 3.2^3 + 4.2^4 + 5.2^5 + 6.2^6 + 7.2^7 + 8.2^8 =$$

$$= 24 + 64 + 160 + 384 + 896 + 2048 = 3576$$

Exemplo 3.2 Temos:

$$2 + 4 + 8 + 16 + 32 + 64 = \sum_{i=1}^{6} 2^i$$

$$1 + 3 + 5 + \ldots + 29 = \sum_{j=1}^{15} (2j - 1)$$

3.2 PROPRIEDADES DOS SOMATÓRIOS

Teorema 3.1 $\sum_{i=1}^{n} (a_i + b_i) = \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i$

Demonstração:

Com efeito, desenvolvendo o primeiro membro, temos:

$$\sum_{i=1}^{n} (a_i+b_i) = (a_1+b_1) + (a_2+b_2) + \ldots + (a_n+b_n) =$$

$$= (a_1+a_2+\ldots+ a_n) + (b_1+b_2+\ldots+ b_n) =$$

$$= \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i$$

Teorema 3.2 $\sum_{i=1}^{n} a = na$

Demonstração:

Seja $a_i = a$ para $i = 1,2,\ldots,n$. Então, temos:

$$\sum_{i=1}^{n} a = \sum_{i=1}^{n} a_i = a_1 + a_2 +\ldots+ a_n = a + a +\ldots+ a = na$$

Teorema 3.3 $\sum_{i=1}^{n} (a_i + a) = \sum_{i=1}^{n} a_i + na$

Demonstração:

Consoante os dois teoremas anteriores, temos:

$$\sum_{i=1}^{n} (a_i + a) = \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} a = \sum_{i=1}^{n} a_i + na$$

<u>Teorema 3.4</u> $\sum_{i=1}^{n} ka_i = k \sum_{i=1}^{n} a_i$

<u>Demonstração:</u>

Com efeito, desenvolvendo o primeiro membro, temos:

$$\sum_{i=1}^{n} ka_i = ka_1 + ka_2 + \ldots + ka_n = k(a_1 + a_2 + \ldots + a_n) = k \sum_{i=1}^{n} a_i$$

<u>Exémplo 3.3</u> Calcular $\sum_{i=1}^{20} (5i + 2)$

Consoante os teoremas anteriores temos, sucessivamente:

$$\sum_{i=1}^{20} (5i+2) = \sum_{i=1}^{20} 5i + \sum_{i=1}^{20} 2 = 5 \sum_{i=1}^{20} i + 20.2 =$$

$$= 5(1 + 2 + \ldots + 20) + 40 =$$

$$= 5 . \frac{1}{2} (1 + 20)20 + 40 = 5.210 + 40 = 1090$$

3.3 SOMATÓRIOS DUPLOS

<u>Teorema 3.5</u> $\sum_{i,j=1}^{n} a_{ij} = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij}$

Demonstração:

Com efeito, desenvolvendo o primeiro membro, temos:

$$\sum_{i,j=1}^{n} a_{ij} = a_{11} + a_{12} + \ldots + a_{1n} + a_{21} + a_{22} + \ldots + a_{2n} + \\ + \ldots + a_{n1} + a_{n2} + \ldots + a_{nn}$$

ou seja:

$$\sum_{i,j=1}^{n} a_{ij} = \sum_{j=1}^{n} a_{1j} + \sum_{j=1}^{n} a_{2j} + \ldots + \sum_{j=1}^{n} a_{nj} = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij}$$

Teorema 3.6 $\quad \sum_{j=1}^{m} \sum_{i=1}^{n} a_i b_j = \sum_{i=1}^{n} a_i \cdot \sum_{j=1}^{m} b_j$

Demonstração:

Com efeito, pelo teorema 3.4, temos:

$$\sum_{j=1}^{m} \sum_{i=1}^{n} a_i b_j = \sum_{j=1}^{m} \left[\sum_{i=1}^{n} a_i b_j \right] = \sum_{j=1}^{m} \left[b_j \sum_{i=1}^{n} a_i \right] =$$

$$= \sum_{i=1}^{n} a_i \cdot \sum_{j=1}^{m} b_j$$

Exemplo 3.4 Calcular $\sum_{j=1}^{2} \sum_{i=1}^{3} 2^i 3^j$

Consoante o teorema 3.6, temos:

$$\sum_{j=1}^{2} \sum_{i=1}^{3} 2^i 3^j = \sum_{i=1}^{3} 2^i . \sum_{j=1}^{2} 3^j = (2 + 2^2 + 2^3)(3 + 3^2) =$$

$$= 14.12 = 168$$

3.4 PRODUTÓRIOS

Sejam os $n > 1$ inteiros $a_1, a_2, \ldots, a_n$. Para indicar, de modo abreviado, o *produto* $a_1 a_2 \ldots a_n$ desses n inteiros usa-se a notação:

$$\prod_{i=1}^{n} a_i$$

que se lê: "produtório de a_i de 1 a n".

Em particular, para $n = 2, 3, \ldots$, temos:

$$\prod_{i=1}^{2} a_i = a_1 a_2, \qquad \prod_{i=1}^{3} a_i = a_1 a_2 a_3, \ \ldots$$

A letra i chama-se o *índice do produtório* e pode ser substituida por qualquer outra diferente de a e de n - é um *índice mudo*. E os inteiros 1 e n que figuram abaixo e acima da letra grega maiúscula Π (pi) chamam-se respectivamente *limite inferior* e *limite superior* do índice i.

O número de *fatores* de um produtório é sempre igual à diferença entre os limites superior e inferior do seu índice mais uma unidade.

Se m e n são dois inteiros, com $m \leq n$, então, por definição:

$$\prod_{i=m}^{n} a_i = a_m . a_{m+1} . a_{m+2} \cdots a_n$$

Exemplo 3.5 Temos:

$$\prod_{i=1}^{6} 3i = (3 .1)(3.2)(3.3)(3.4)(3.5)(3.6) =$$
$$= 3.6.9.12.15.18 = 524880$$

$$\prod_{j=1}^{4} (5j - 3) = (5.1 - 3)(5.2 - 3)(5.3 - 3)(5.4 - 3) =$$
$$= 2.7.12.17 = 2856$$

Exemplo 3.6 Temos:

$$3.9.27.81.243.729 = \prod_{i=1}^{6} 3^i$$

$$1.3.5.7....31 = \prod_{j=1}^{16} (2j - 1)$$

$$1.2.3...(n-1)n = n! = \prod_{i=1}^{n} i$$

3.5 PROPRIEDADES DOS PRODUTÓRIOS

Teorema 3.7

$$\prod_{i=1}^{n} a_i b_i = \prod_{i=1}^{n} a_i . \prod_{i=1}^{n} b_i$$

Demonstração:

Com efeito, desenvolvendo o primeiro membro, temos:

$$\prod_{i=1}^{n} a_i b_i = (a_1 b_1)(a_2 b_2)\ldots(a_n b_n) = (a_1 a_2 \ldots a_n)(b_1 b_2 \ldots$$

$$\ldots b_n) = \prod_{i=1}^{n} a_i \cdot \prod_{i=1}^{n} b_i$$

Teorema 3.8 $\prod_{i=1}^{n} a = a^n$

Demonstração:

Seja $a_i = a$ para $i = 1,2,\ldots,n$. Então, temos:

$$\prod_{i=1}^{n} a = \prod_{i=1}^{n} a_i = a_1 a_2 \ldots a_n = a.a \ldots a = a^n$$

Teorema 3.9 $\prod_{i=1}^{n} ka_i = k^n \prod_{i=1}^{n} a_i$

Demonstração:

Com efeito, desenvolvendo o primeiro membro, temos:

$$\prod_{i=1}^{n} ka_i = (ka_1)(ka_2)\ldots(ka_n) = k^n(a_1 a_2 \ldots a_n) = k^n \prod_{i=1}^{n} a_i$$

Exemplo 3.7 Calcular $\prod_{i=1}^{4} (2i + 1)^2$

Consoante o teorema 3.7, temos:

$$\prod_{i=1}^{4} (2i+1)^2 = \left[\prod_{i=1}^{4} (2i+1)\right]^2 = (3.5.7.9)^2 = 945^2 = \\ = 893025$$

<u>Exemplo 3.8</u> Demonstrar: $\prod_{i,j=1}^{n} a_{ij} = \prod_{i=1}^{n} \prod_{j=1}^{n} a_{ij}$

Com efeito, desenvolvendo o primeiro membro, temos:

$$\prod_{i,j=1}^{n} a_{ij} = (a_{11}a_{12}\cdots a_{1n})(a_{21}a_{22}\cdots a_{2n})\cdots(a_{n1}a_{n2}\cdots \\ \cdots a_{nn}) = \prod_{j=1}^{n} a_{1j} \cdot \prod_{j=1}^{n} a_{2j} \cdots \prod_{j=1}^{n} a_{nj} = \prod_{i=1}^{n} \prod_{j=1}^{n} a_{ij}.$$

3.6 TEOREMA DO BINÔMIO

Para todo inteiro positivo <u>n</u> o desenvolvimento de $(a+b)^n$ é dado pela fórmula:

$$(a + b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \ldots + \\ + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n \qquad (1)$$

ou seja, sob forma condensada:

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

<u>Demonstração:</u>

Usando o "Teorema da indução matemática", a fórmula é verdadeira para n = 1, pois, temos:

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

Suponhamos, agora, que a fórmula *subsiste* para o inteiro positivo m *(hipótese de indução)*. Então, teremos:

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

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

Somando ordenadamente essas duas igualdades, obtemos:

$$(a+b)^{m+1} = a^{m+1} + \sum_{k=1}^{m} \left[\binom{m}{k} + \binom{m}{k-1} \right] a^{m+1-k} b^k + b^{m+1} =$$

$$= \sum_{k=0}^{m+1} \binom{m+1}{k} a^{m+1-k} b^k$$

isto é, a fórmula *subsiste* para o inteiro positivo m+1 e, portanto, é verdadeira para todo inteiro positivo m.

Exemplo 3.9 Desenvolver: $(a+b)^2$, $(a+b)^3$ e $(a+b)^4$.

Fazendo sucessivamente $n = 2,3,4$ na fórmula (1), obtemos:

$$(a + b)^2 = \binom{2}{0} a^2 + \binom{2}{1} ab + \binom{2}{2} b^2 =$$

$$= a^2 + 2ab + b^2$$

$$(a + b)^3 = \binom{3}{0} a^3 + \binom{3}{1} a^2 b + \binom{3}{2} ab^2 + \binom{3}{3} b^3 =$$

$$= a^3 + 3a^2 b + 3ab^2 + b^3$$

$$(a + b)^4 = \binom{4}{0}a^4 + \binom{4}{1}a^3b + \binom{4}{2}a^2b^2 + \binom{4}{3}ab^3 + \binom{4}{4}b^4 =$$
$$= a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$$

<u>Exemplo 3.10</u> Calcular a soma:

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n}$$

Basta fazer $a = b = 1$ na fórmula (1), o que dá:

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n} = (1+1)^n = 2^n$$

Assim, p.ex.:

$$\binom{5}{0} + \binom{5}{1} + \binom{5}{2} + \binom{5}{3} + \binom{5}{4} + \binom{5}{5} = 2^5 = 32$$

Portanto, a soma dos coeficientes do desenvolvimento de $(a + b)^n$ é igual a 2^n.

3.7 TRIÂNGULO DE PASCAL

A *tabela* abaixo, formada com os números binomiais de *numeradores*

$$0,1,2,3, \ldots,$$

é o que se chama *triângulo de PASCAL:*

$$\binom{0}{0}$$

$$\binom{1}{0} \quad \binom{1}{1}$$

$$\binom{2}{0} \quad \binom{2}{1} \quad \binom{2}{2}$$

$$\binom{3}{0} \quad \binom{3}{1} \quad \binom{3}{2} \quad \binom{3}{3}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\binom{n-1}{0} \quad \binom{n-1}{1} \quad \binom{n-1}{2} \quad \binom{n-1}{3} \quad \cdots \quad \binom{n-1}{n-1}$$

$$\binom{n}{0} \quad \binom{n}{1} \quad \binom{n}{2} \quad \binom{n}{3} \quad \cdots \quad \binom{n}{n-1} \quad \binom{n}{n}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

Substituindo os números binomiais pelos seus respectivos valores, o triângulo de PASCAL escreve-se:

1							
1	1						
1	2	1					
1	3	3	1				
1	4	6	4	1			
1	5	10	10	5	1		
1	6	15	20	15	6	1	
1	7	21	35	35	21	7	1

.....

Observe-se que, no *triângulo de PASCAL:*

(i) o primeiro elemento é 1;

(ii) cada linha tem um elemento a mais que a linha anterior;

(iii) todas as linhas começam e terminam por 1, visto que

$$\binom{n}{0} = \binom{n}{n} = 1$$

(iv) os elementos da linha de ordem $n+1$ são precisamente os coeficientes do desenvolvimento de $(a+b)^n$.

Assim, p.ex., os elementos da sétima linha são os coeficientes do desenvolvimento de $(a+b)^6$.

3.8 PROPRIEDADES DO TRIÂNGULO DE PASCAL

O *triângulo de PASCAL* goza de inúmeras propriedades, dentre as quais destacam-se as seguintes:

(I) Dois elementos de uma mesma linha, equidistantes dos extremos, são iguais.

É consequência da fórmula $\binom{m}{k} = \binom{m}{m-k}$: dois números binomiais complementares são iguais.

(II) A soma dos elementos da linha de ordem $n+1$ é igual a 2^n.

É consequência da fórmula:

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n-1} + \binom{n}{2} = 2^n$$

(III) Cada elemento de uma linha, a partir do segundo, é a soma do elemento que lhe fica acima com o que está à esquerda deste último.

É consequência da *relação de STIFEL:*

$$\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k}$$

Esta propriedade permite a construção rápida e fácil do *triângulo de PASCAL.*

(IV) A soma de um número qualquer de elementos consecutivos de uma *coluna*, a partir do primeiro, é igual ao elemento que se encontra na interseçao da linha e da coluna imediatamente posteriores aquelas a que pertence o último dos elementos considerados.

Esta propriedade resulta da fórmula:

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-2}{k-1} + \ldots + \binom{k}{k-1} + \binom{k-1}{k-1}$$

Assim, p.ex., a soma dos n primeiros elementos da *segunda coluna:*

$$\binom{1}{1}, \binom{2}{1}, \binom{3}{1}, \ldots, \binom{n-1}{1}, \binom{n}{1}$$

é igual a $\binom{n+1}{2}$, isto é:

$$1 + 2 + 3 + \ldots + (n-1) + n = \frac{n(n+1)}{2}$$

(V) A soma de um número qualquer de elementos consecutivos de uma mesma *diagonal*, a partir de um elemento da primeira coluna, é igual ao elemento que se encontra na mesma coluna do último elemento considerado e imediatamente abaixo deste.

Esta propriedade decorre da fórmula:

$$\binom{n}{n-k} = \binom{n-1}{n-k} + \binom{n-2}{n-k-1} + \ldots + \binom{k}{1} + \binom{k-1}{0}$$

Assim, p.ex., são elementos consecutivos de uma mesma *diagonal:*

$$\binom{1}{0}, \binom{2}{1}, \binom{3}{2}, \ldots, \binom{n}{n-1}$$

e, portanto:

$$\binom{1}{0} + \binom{2}{1} + \binom{3}{2} + \ldots + \binom{n}{n-1} = \binom{n+1}{n-1}$$

3.9. NÚMEROS TRIANGULARES

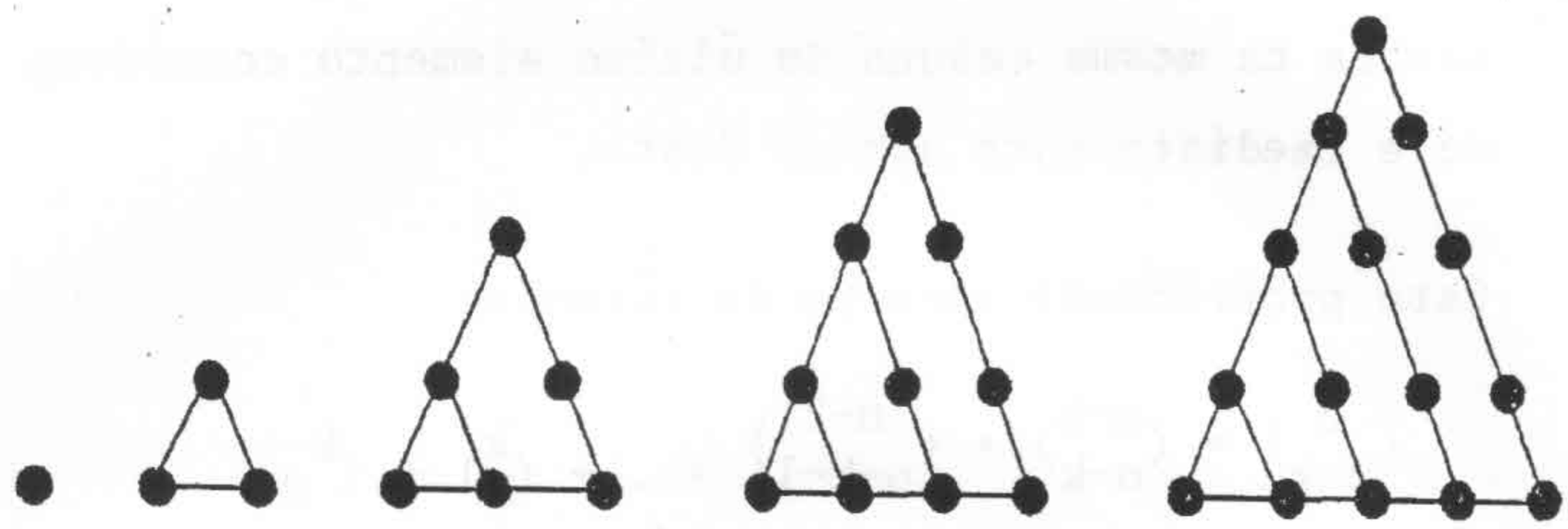
Os inteiros que formam a *terceira coluna* do *triângulo de PASCAL:*

$$1 = 1, \quad 3 = 1 + 2, \quad 6 = 1 + 2 + 3$$

$$10 = 1 + 2 + 3 + 4, \quad 15 = 1 + 2 + 3 + 4 + 5, \ldots$$

cada um dos quais é a soma de inteiros consecutivos começando por 1, chamam-se *números triangulares*, porque cada

um deles dá o número de pontos que podem ser dispostos em forma de triângulo equilátero, conforme mostram as figuras abaixo:



Denotando o n-ésimo número triangular por t_n, as propriedades do triângulo de PASCAL permitem afirmar que t_n tem para expressão:

$$t_n = \binom{n+1}{2} = \frac{n(n+1)}{2}$$

e que a soma S_t dos n primeiros números triangulares é dada pela fórmula:

$$S_t = \binom{n+2}{3} = \frac{n(n+1)(n+2)}{6}$$

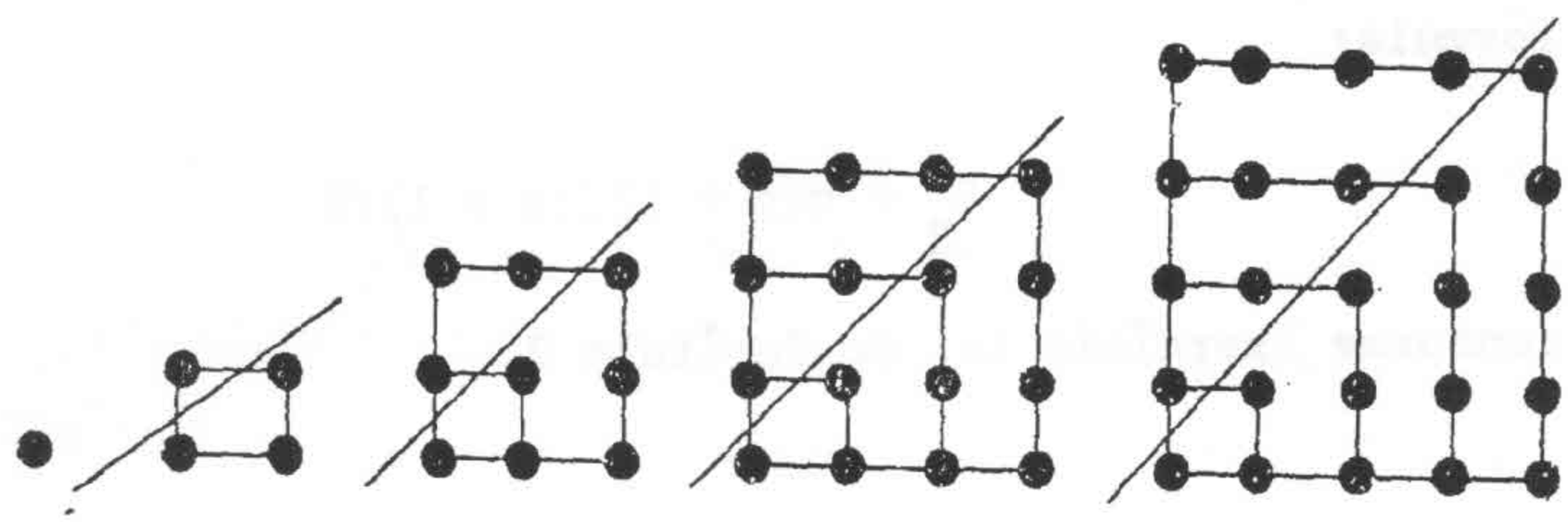
Teorema 3.10 A soma de dois números triangulares consecutivos é um quadrado perfeito.

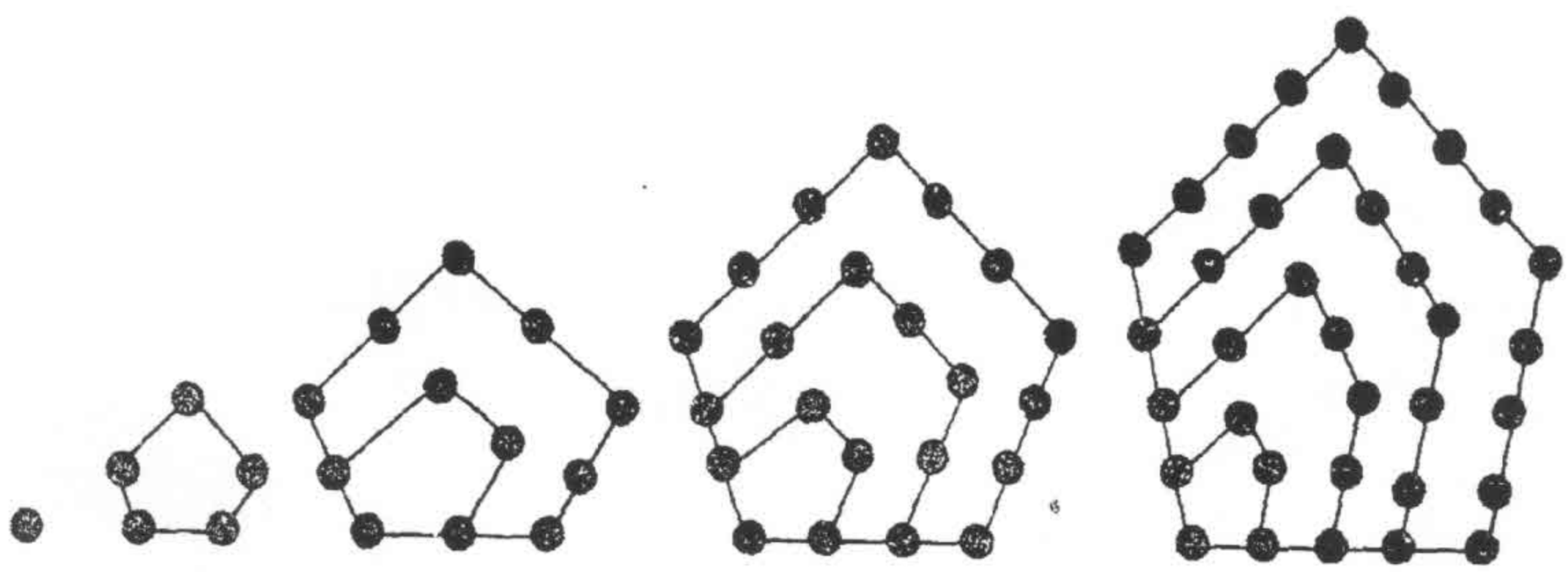
Demonstração:

Com efeito:

$$t_{n-1} + t_n = \frac{(n-1)n}{2} + \frac{n(n+1)}{2} = n^2$$

NOTA. Os pitagóricos relacionaram os inteiros com a Geometria, introduzindo os *números poligonais* : *números triangulares*, *números quadráticos*, *números pentagonais*, etc. A razão desta nomenclatura geométrica resulta da representação dos números poligonais mediante pontos dispostos em forma de triângulos, quadrados, pentágonos, etc., como mostram as figuras que se seguem:





Denotando o n-ésimo número quadrático por q_n, é imediato que $q_n = n^2$, e temos (Teorema 3.10):

$$q_n = t_{n-1} + t_n$$

isto é, o n-ésimo número quadrático é a soma do n-ésimo número triangular e do seu antecessor.

Este resultado os pitagóricos conheciam, e o demonstraram separando os pontos e contando-os, no modo indicado nas figuras.

A soma S_q dos n primeiros números quadráticos é dado pela fórmula:

$$S_q = n(n + 1)(2n + 1)/6$$

conforme Exercício 1a. do Capítulo 2.

EXERCÍCIOS

1. Calcular:

(a) $\sum_{i=1}^{5} 3^{i}$ (b) $\sum_{i=3}^{7} 6$

(c) $\sum_{j=1}^{4} (j+1)(j+2)$ (d) $\sum_{k=1}^{3} k^{2k}$

2. Calcular:

(a) $\prod_{i=1}^{3} (3+i^2)$ (b) $\prod_{k=1}^{3} 5$

(c) $\prod_{j=2}^{6} (j-1)(j+1)$ (d) $\prod_{n=3}^{7} n/2^{n}$

3. Usando o símbolo de *somatório*, escrever as seguintes expressões:

(a) $a_1b_2 + a_2b_3 + a_3b_4 + a_4b_5$

(b) $3.4.5 + 4.5.6 + 5.6.7 + \ldots + k(k+1)(k+2)$

(c) $a_{21}b_{13} + a_{22}b_{23} + a_{23}b_{33} + a_{24}b_{43} + a_{25}b_{53}$

4. Dizer se é *verdadeiro* (V) ou *falso* (F):

(a) $\sum_{i=1}^{n} (i+3) = \sum_{i=4}^{n+3} i$ (b) $\sum_{i=1}^{n} (2+i) = 2+ \sum_{i=1}^{n} i$

(c) $\prod_{i=1}^{n} a_i^2 = (\prod_{i=1}^{n} a_i)^2$ (d) $\sum_{i=0}^{5} a_i = \sum_{i=1}^{5} a_i$

5. Demonstrar:

$$\prod_{i=1}^{m} \prod_{j=1}^{n} a_{ij} = \prod_{j=1}^{n} \prod_{i=1}^{m} a_{ij}$$

6. Demonstrar as seguintes propriedades dos *números triangulares:*

(a) Um número é *triangular* se e somente se é da forma $n(n + 1)/2$, onde $\underline{n}$ é um inteiro positivo.

(b) O inteiro $\underline{n}$ é um *número triangular* se e somente se $8n+1$ é um *quadrado perfeito.*

(c) Se $\underline{n}$ é um *número triangular*, então $9n+1$, $25n+3$ e $49n+6$ também são *números triangulares.*

7. Na sequência dos números triangulares, achar:

(a) dois números triangulares cuja soma e diferença também sejam números triangulares;

(b) três números triangulares consecutivos cujo produto seja um quadrado perfeito;

(c) três números triangulares consecutivos cuja soma seja um quadrado perfeito.

8. Demonstrar:

(a) $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} + \ldots + (-1)^n \binom{n}{n} = 0, \; n \geq 1$

(b) $\binom{n}{1} + 2\binom{n}{2} + 3\binom{n}{3} + \ldots + n\binom{n}{n} = n.2^{n-1}, \; n \geq 1$

(c) $\binom{n}{0} + 2\binom{n}{1} + 2^2\binom{n}{2} + \ldots + 2^n\binom{n}{n} = 3^n, \; n \geq 1$

(d) $\binom{2}{2} + \binom{3}{2} + \binom{4}{2} + \ldots + \binom{n}{2} = \binom{n+1}{3}, \; n \geq 2$

9. Calcular o *termo independente* de $\underline{x}$ no desenvolvimento de

$$\left(\sqrt{x} + \frac{2}{x}\right)^9$$

10. No desenvolvimento de $(a + b)^n$ os coeficientes do 3º e do 8º termos são *iguais*. Calcular $\underline{n}$.

CAPÍTULO 4

DIVISIBILIDADE

4.1 RELAÇÃO DE DIVISIBILIDADE EM Z

Definição 4.1 Sejam a e b dois inteiros, com $a \neq 0$. Diz-se que a *divide* b se e somente se existe um inteiro q tal que $b = aq$.

Se a *divide* b também se diz que a é um *divisor* de b, que b é um *múltiplo* de a, que a é um *fator* de b ou que b é *divisivel* por a.

Com a notação "$a|b$" indica-se que $a \neq 0$ *divide* b e, portanto, a notação "$a \nmid b$" significa que $a \neq 0$ *não divide* b.

A relação "a divide b ($a|b$)" denomina-se *relação de divisibilidade em* Z.

Se a é um *divisor* de b, então $-a$ também é um *divisor* de b, porque a igualdade $b = aq$ implica $b = (-a)(-q)$, de modo que os *divisores* de um inteiro qualquer são dois a dois iguais em valor absoluto e de sinais opostos (simé-

tricos).

Assim, p.ex.:

$2|6$, porque $6 = 2.3$

$-5|30$, porque $30 = (-5)(-6)$

$7|-21$, porque $-21 = 7(-3)$

$3\nmid 10$, porque não existe $q \in Z$ tal que $10 = 3z$

<u>Teorema 4.1</u> Quaisquer que sejam os inteiros <u>a</u>, <u>b</u> e <u>c</u>, tem se:

(1) $a|0$, $1|a$ e $a|a$

(2) Se $a|1$, então $a = \pm 1$

(3) Se $a|b$ e se $c|d$, então $ac|bd$

(4) Se $a|b$ e se $b|c$, então $a|c$

(5) Se $a|b$ e se $b|a$, então $a = \pm b$

(6) Se $a|b$, com $b \neq 0$, então $|a| \leq |b|$

(7) Se $a|b$ e se $a|c$, então $a|(bx+cy)$, $\forall\, x,y \in Z$

<u>Demonstração:</u>

(1) Com efeito:

$$0 = a.0, \quad a = 1.a, \quad a = a.1$$

(2) Com efeito, se $a|1$, então $1 = aq$, com $q \in Z$, o que

implica $a = 1$ e $q = 1$ ou $a = -1$ e $q = -1$, isto é: $a = \pm 1$.

(3) Com efeito:

$$a|b \Longrightarrow b = aq, \quad \text{com} \quad q \in Z$$

$$c|d \Longrightarrow d = cq_1, \quad \text{com} \quad q_1 \in Z$$

Portanto:

$$bd = (ac)(qq_1) \Longrightarrow ac|bd$$

(4) Com efeito:

$$a|b \Longrightarrow b = aq, \quad \text{com} \quad q \in Z$$

$$b|c \Longrightarrow c = bq_1, \quad \text{com} \quad q_1 \in Z$$

Portanto:

$$c = a(qq_1) \Longrightarrow a|c$$

(5) Com efeito:

$$a|b \Longrightarrow b = aq, \quad \text{com} \quad q \in Z$$

$$b|a \Longrightarrow a = bq_1, \quad \text{com} \quad q_1 \in Z$$

Portanto:

$$a = a(qq_1) \Longrightarrow qq_1 = 1 \Longrightarrow q_1 | 1$$

$$\Longrightarrow q_1 = \pm 1 \Longrightarrow a = \pm b$$

(6) Com efeito:

$$a|b,\ b \neq 0 \Longrightarrow b = aq,\quad q \neq 0 \qquad |b| = |a|\,|q|$$

Como $q \neq 0$, segue-se que $|q| \geq 1$ e, portanto:

$$|b| \geq |a|$$

(7) Com efeito:

$$a|b \Longrightarrow b = aq, \quad \text{com} \quad q \in Z$$

$$a|c \Longrightarrow c = aq_1, \quad \text{com} \quad q_1 \in Z$$

Portanto, quaisquer que sejam os inteiros $\underline{x}$ e $\underline{y}$:

$$bx+cy = aqx+aq_1y = a(qx+q_1y) \Longrightarrow a|(bx+cy)$$

Esta propriedade (7) admite uma óbvia generalização; isto é, se

$$a|b_k, \quad \text{para} \quad k = 1, 2, \ldots, n$$

então, quaisquer que sejam os inteiros

$$x_1, x_2, \ldots, x_n:$$

$$a|(b_1x_1 + b_2x_2 + \ldots + b_nx_n)$$

Consoante as propriedades (1) e (4), a relação de divisibilidade Z é *reflexiva* e *transitiva*, mas *não é simétrica*, porque, p.ex., $3|6$ e $6 \nmid 3$.

4.2 CONJUNTO DOS DIVISORES DE UM INTEIRO

O conjunto de todos os *divisores* de um inteiro qualquer $\underline{a}$ indica-se por $D(a)$, isto é:

$$D(a) = \{x \in Z^* \mid x|a\}$$

onde Z^* denota o conjunto dos inteiros *não nulos* ($\neq 0$). Assim, p.ex.:

$$D(0) = \{x \in Z^* \mid x|0\} = Z^*$$

$$D(1) = \{x \in Z^* \mid x|1\} = \{-1,1\}$$

$$D(2) = \{x \in Z^* \mid x|2\} = \{\pm 1, \pm 2\}$$

$$D(-8) = \{x \in Z^* \mid x|-8\} = \{\pm 1, \pm 2, \pm 4, \pm 8\}$$

É imediato que, para todo inteiro $\underline{a}$, se tem $D(a) = D(-a)$, e como

$$a = a.1 = (-a).(-1)$$

segue-se que 1, -1, $\underline{a}$ e $-\underline{a}$ são *divisores* de $\underline{a}$, denominados *divisores triviais* de $\underline{a}$. Em particular, o inteiro 1 (ou -1) só admite *divisores triviais*.

Qualquer que seja o inteiro $a \neq 0$, se $x|a$, então:

$$-a \leqslant x \leqslant a \Longrightarrow D(a) \subset [-a,a]$$

e isto significa que qualquer inteiro $a \neq 0$ tem um número *finito* de divisores.

4.3 DIVISORES COMUNS DE DOIS INTEIROS

<u>Definição 4.2</u> Chama-se *divisor comum* de dois inteiros $\underline{a}$ e $\underline{b}$ todo inteiro $d \neq 0$ tal que $d|a$ e $d|b$.

Em outros termos, *divisor comum* de dois inteiros a e b é todo inteiro $d \neq 0$ que pertence simultaneamente aos conjuntos $D(a)$ e $D(b)$.

O conjunto de todos os *divisores comuns* a dois inteiros a e b indica-se por $D(a,b)$. Portanto, simbolicamente:

$$D(a,b) = \{ x \in Z^* \mid x|a \quad e \quad x|b \}$$

ou seja:

$$D(a,b) = \{ x \in Z^* \mid x \in D(a) \quad e \quad x \in D(b) \}$$

e, portanto:

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

A *interseção* ($\cap$) é uma *operação comutativa*, de modo que $D(a,b)$ não depende da *ordem* dos inteiros dados a e b, isto é: $D(a,b) = D(b,a)$.

Como -1 e 1 são *divisores comuns* de dois inteiros quaisquer a e b, segue-se que o conjunto $D(a,b)$ dos *divisores comuns* de a e b *nunca é vazio*: $D(a,b) \neq \phi$. Em particular, se $a = b = 0$, então todo inteiro não nulo é um *divisor comum* de a e b, isto é: $D(a,b) = Z^*$.

Exemplo 4.1 Sejam os inteiros $a = 12$ e $b = -15$. Temos:

$$D(12) = \{ \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12 \}$$

$$D(-15) = \{ \pm 1, \pm 3, \pm 5, \pm 15 \}$$

Portanto:

$$D(12,-15) = D(12) \cap D(-15) = \{ \pm 1, \pm 3 \}$$

4.4 ALGORITMO DA DIVISÃO

Teorema 4.2 Se a e b são dois inteiros, com $b > 0$, então *existem* e são *únicos* os inteiros q e r que satisfazem às condições:

$$a = bq + r \quad e \quad 0 \leqslant r < b$$

Demonstração:

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

$$S = \{ a - bx \mid x \in Z,\ a - bx \geqslant 0 \}$$

Este conjunto S não é vazio ($S \neq \phi$), porque, sendo $b > 0$, temos $b \geqslant 1$ e, portanto, para $x = -|a|$, resulta:

$$a - bx = a + b|a| \geqslant a + |a| \geqslant 0$$

Assim sendo, pelo *"Princípio da boa ordenação"*, existe o *elemento mínimo* r de S tal que

$$r \geqslant 0 \quad e \quad r = a - ba \quad ou \quad a = bq + r, \quad com \quad q \in Z$$

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

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

isto é, r não seria o *elemento mínimo* de S.

Para demonstrar a *unicidade* de q e r, suponhamos que *existem* dois outros inteiros q_1 e r_1 tais que

$$a = bq_1 + r_1 \quad e \quad 0 \leqslant r_1 < b$$

Então, teremos:

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

Por outro lado, temos:

$$-b < -r \leqslant 0 \quad e \quad 0 \leqslant r_1 < b$$

o que implica:

$$-b < r_1 - r < b, \quad \text{isto é:} \quad |r_1 - r| < b$$

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

Corolário 4.1 Se a e b são dois inteiros, com $b \neq 0$, *existem* e são *únicos* os inteiros q e r que satisfazem as condições:

$$a = bq + r \quad e \quad 0 \leq r < |b|$$

Demonstração:

Com efeito, se $b > 0$, nada há que demonstrar, e se $b < 0$,

então $|b| > 0$, e por conseguinte *existem* e são *únicos* os inteiros q_1 e $\underline{r}$ tais que

$$a = |b|q_1 + r \quad e \quad 0 \leqslant r < |b|$$

ou seja, por ser $|b| = -b$:

$$a = b(-q_1) + r \quad e \quad 0 \leqslant r < |b|$$

Portanto, *existem* e são *únicos* os inteiros $q = -q_1$ e $\underline{r}$ tais que

$$a = bq + r \quad e \quad 0 \leqslant r < |b|$$

Os inteiros $\underline{q}$ e $\underline{r}$ chamam-se respectivamente o *quociente* e o *resto* na divisão de $\underline{a}$ por $\underline{b}$.

Observe-se que $\underline{b}$ é *divisor* de $\underline{a}$ se e somente se o *resto* $r = 0$. Neste caso, temos $a = bq$ e o *quociente* $\underline{q}$ na divisão exata de $\underline{a}$ por $\underline{b}$ indica-se também por $\frac{a}{b}$ ou

$$a/b \ (q = \frac{a}{b} = a/b),$$

que se lê "a sobre b".

<u>Exemplo 4.2</u> Achar o *quociente* $\underline{q}$ e o *resto* $\underline{r}$ na divisão de $a = 59$ por $b = -14$ que satisfazem às condições do *algoritmo da divisão*.

Efetuando a divisão usual dos *valores absolutos* de $\underline{a}$ e $\underline{b}$, obtemos:

$$59 = 14.4 + 3$$

o que implica:

$$59 = (-14)(-4) + 3 \quad \text{e} \quad 0 \leqslant 3 < |-14|$$

Logo, o *quociente* $q = -4$ e o *resto* $r = 3$.

<u>Exemplo 4.3</u> Achar o *quociente* <u>q</u> e o *resto* <u>r</u> na divisão de $a = -79$ por $b = 11$ que satisfazem às condições do *algoritmo da divisão*.

Efetuando a divisão usual dos *valores absolutos* de <u>a</u> e <u>b</u>, obtemos:

$$79 = 11.7 + 2$$

o que implica:

$$-79 = 11(-7) - 2$$

Como o termo $r = -2 < 0$ não satisfaz à condição $0 \leqslant r < 11$, somando e subtraindo o valor 11 de <u>b</u> ao segundo membro da igualdade anterior, obtemos:

$$-79 = 11(-7) - 11 + 11 - 2 = 11(-8) + 9$$

com $0 \leqslant 9 < 11$. Logo, o *quociente* $q = -8$ e o *resto* $r = 9$.

<u>Exemplo 4.4</u> Sejam os inteiros $a = 1, -2, 61, -59$ e $b = -7$. Temos:

$$1 = (-7).0 + 1 \quad \text{e} \quad 0 \leqslant 1 < |-7| \Longrightarrow q = 0 \text{ e } r = 1$$

$$-2 = (-7).1 + 5 \quad \text{e} \quad 0 \leqslant 5 < |-7| \Longrightarrow q = 1 \text{ e } r = 5$$

$$61 = (-7)(-8) + 5 \quad e \quad 0 \leqslant 5 < |-7| \Longrightarrow q = -8 \text{ e } r = 5$$

$$-59 = (-7).9 + 4 \quad e \quad 0 \leqslant 4 < |-7| \Longrightarrow q = 9 \quad e \quad r = 4$$

4.5 PARIDADE DE UM INTEIRO

Na divisão de um inteiro qualquer a por b = 2 os possíveis *restos* são r = 0 e r = 1. Se r = 0, então o inteiro a = 2q e é denominado *par*; e se r = 1, então o inteiro a = 2q + 1 e é denominado *ímpar*.

Observe-se que

$$a^2 = (2q)^2 = 4q^2 \quad \text{ou} \quad a^2 = 4(q^2 + q) + 1$$

de modo que na divisão do quadrado a^2 de um inteiro qualquer a por 4 o *resto* é 0 ou 1.

Exemplo 4.5 Mostrar que o *quadrado* de qualquer inteiro *ímpar* é da forma 8k + 1.

Com efeito, pelo algoritmo da divisão, qualquer inteiro é de uma das seguintes formas:

$$4q,\ 4q+1,\ 4q + 2,\ 4q + 3$$

Nesta classificação, somente os inteiros das formas 4q+1 e 4q+3 são *ímpares* e, portanto, os seus *quadrados* são da forma:

$$(4q+1)^2 = 8(2q^2 + q) + 1 = 8k + 1$$

$$(4q+3)^2 = 8(2q^2 + 3q + 1) + 1 = 8k + 1$$

Assim, p.ex., 7 e 13 são inteiros *ímpares*, e temos:

$$7^2 = 49 = 8.6 + 1$$

$$13^2 = 169 = 8.21 + 1$$

EXERCÍCIOS

1. Mostrar que, se $a|b$, então $(-a)|b$, $a|(-b)$ e $(-a)|(-b)$.

2. Sejam a, b e c inteiros. Mostrar:

   (a) se $a|b$, então $a|bc$

   (b) se $a|b$ e se $a|c$, então $a^2|bc$

   (c) $a|b$ se e somente se $ac|bc$ $(c \neq 0)$

3. Verdadeiro ou falso:

   se $a|(b+c)$, então $a|b$ ou $a|c$.

4. Mostrar que, se a é um inteiro qualquer, então um dos inteiros: a, $a+2$, $a+4$ é divisível por 3.

5. Sendo a um inteiro qualquer, mostrar:

   (a) $2|a(a+1)$ (b) $3|a(a+1)(a+2)$

6. Mostrar que um inteiro qualquer da forma $6k+5$ também é da forma $3k+2$.

7. Mostrar que todo inteiro *ímpar* é da forma $4k+1$ ou $4k+3$.

8. Mostrar que o *quadrado* de um inteiro qualquer é da forma $3k$ ou $3k+1$.

9. Mostrar que o *cubo* de um inteiro qualquer é de uma das formas: $9k$, $9k+1$ ou $9k+8$.

10. Mostrar que $n(n+1)(2n+1)/6$ é um inteiro, qualquer que seja o inteiro positivo $\underline{n}$.

11. Mostrar que, se $a|(2x - 3y)$ e se $a|(4x - 5y)$, então $a|y$.

12. Sendo $\underline{a}$ e $\underline{b}$ dois inteiros quaisquer, mostrar que os inteiros $\underline{a}$ e $a+2b$ têm sempre a mesma *paridade*.

13. Sendo $\underline{m}$ e $\underline{n}$ dois inteiros quaisquer, mostrar que os inteiros $m+n$ e $m-n$ têm sempre a mesma *paridade*.

14. Determinar os inteiros positivos que divididos por 17 deixam um resto igual ao quadrado do quociente.

15. Achar inteiros $\underline{a}$, $\underline{b}$ e $\underline{c}$ tais que $a|bc$, mas $a \nmid b$ e $a \nmid c$.

16. Verdadeiro ou falso: se $a|c$ e se $b|c$, então $a|b$.

17. Demonstrar:
    (a) Se $\underline{a}$ é um inteiro *ímpar*, então $24|a(a^2 - 1)$.
    (b) Se $\underline{a}$ e $\underline{b}$ são inteiros *ímpares*, então $8|(a^2 - b^2)$.

18. Mostrar que a diferença entre os cubos de dois inteiros consecutivos nunca é divisível por 2.

19. Na divisão do inteiro $a = 427$ por um inteiro positivo $\underline{b}$ o *quociente* é 12 e o *resto* é $\underline{r}$. Achar o *divisor* $\underline{b}$ e o *resto* $\underline{r}$.

20. Na divisão do inteiro 525 por um inteiro positivo o *resto* é 27. Achar os inteiros que podem ser o *divisor* e o *quociente*.

21. Na divisão de dois inteiros positivos o *quociente* é 16 e o *resto* é o *maior possível*. Achar os dois inteiros, sabendo que a sua soma é 341.

22. Achar os inteiros positivos menores que 150 e que divididos por 39 deixam um resto igual ao quociente.

23. Seja $\underline{d}$ um divisor de $n (d|n)$. Mostrar que $cd|n$ se e somente se $c|(n/d)$.

24. Sejam $\underline{n}$, $\underline{r}$ e $\underline{s}$ inteiros tais que $0 \leqslant r < n$ e $0 \leqslant s < n$. Mostrar que, se $n|(r - s)$, então $r = s$.

25. Mostrar que o produto de dois inteiros *ímpares* é um inteiro *ímpar*.

26. Demonstrar que, se $\underline{m}$ e $\underline{n}$ são inteiros ímpares, então $8|(m^4 + n^4 - 2)$.

27. Demonstrar que $30|(n^5 - n)$.

28. Mostrar que, para todo inteiro $\underline{n}$, existem inteiros $\underline{k}$ e $\underline{r}$ tais que

$$n = 3k+r \quad e \quad r = -1,0,1$$

29. Mostrar que

$$(1 + 2 + \ldots + n) \mid 3(1^2 + 2^2 + \ldots + n^2)$$

para todo $n \geqslant 1$.

30. Mostrar que todo inteiro ímpar, quadrado perfeito, é da forma $4n+1$.

31. Na divisão de 392 por 45, determinar:
    (a) o maior inteiro que se pode somar ao dividendo sem alterar o quociente;
    (b) o maior inteiro que se pode subtrair do dividendo sem alterar o quociente.

32. Numa divisão de dois inteiros, o quociente é 16 e o resto é 167. Determinar o maior inteiro que se pode somar ao dividendo e ao divisor sem alterar o quociente.

33. Achar o maior inteiro de quatro algarismos divisível por 13 e o menor inteiro de cinco algarismos divisível por 15.

34. Achar um inteiro de quatro algarismos, quadrado perfeito, divisível por 27 e terminado em 6.

CAPÍTULO 5

MÁXIMO DIVISOR COMUM

5.1 MÁXIMO DIVISOR COMUM DE DOIS INTEIROS

Definição 5.1 Sejam a e b dois inteiros não conjuntamente nulos ($a \neq 0$ ou $b \neq 0$). Chama-se *máximo divisor comum* de a e b o inteiro *positivo* d ($d > 0$) que satisfaz às condições:

(1) $d|a$ e $d|b$

(2) se $c|a$ e se $c|b$, então $c \leq d$.

Observe-se que, pela condição (1), d é um *divisor comum* de a e b, e pela condição (2), d é o *maior* dentre todos os divisores comuns de a e b.

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

É imediato que o mdc(a,b) = mdc(b,a). Em particular:

(i) o mdc(0,0) *não existe*

(ii) o mdc(a,1) = 1

(iii) se $a \neq 0$, então o $mdc(a,0) = |a|$

(iv) se $a|b$, então o $mdc(a,b) = |a|$

Assim, p.ex.:

$mdc(8,1) = 1$, $mdc(-3,0) = |-3| = 3$

$mdc(-6,12) = |-6| = 6$

Exemplo 5.1 Sejam os inteiros $a = 16$ e $b = 24$. Os *divisores comuns positivos* de 16 e 24 são 1, 2, 4 e 8, e como o *maior* deles é 8, segue-se que o $mdc(16,24) = 8$.

Observe-se que

$$mdc(-16,24) = mdc(16,-24) = mdc(-16,-24) = 8.$$

Exemplo 5.2 Sejam os inteiros $a = -24$ e $b = 60$. Os *divisores comuns positivos* de -24 e 60 são 1,2,3,4,6 e 12, e como o *maior* deles é 12, segue-se que o $mdc(-24,60) = 12$.

5.2 EXISTÊNCIA E UNICIDADE DO MDC

Teorema 5.1 Se $\underline{a}$ e $\underline{b}$ são dois inteiros não conjuntamente nulos ($a \neq 0$ ou $b \neq 0$), então *existe* e é *único* o $mdc(a,b)$; além disso, *existem* inteiros $\underline{x}$ e $\underline{y}$ tais que

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

isto é, o $mdc(a,b)$ é uma *combinação linear* de $\underline{a}$ e $\underline{b}$.

Demonstração:

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

$$S = \{ au + bv \mid au + bv > 0 \quad e \quad u,v \in Z \}$$

Este conjunto S *não é vazio* ($S \neq \phi$), porque, p.ex., se $a \neq 0$, então um dos dois inteiros:

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

é *positivo* e pertence a S. Logo, pelo *"Princípio da boa ordenação", existe* e é *único* o *elemento mínimo* d de S: $\min S = d > 0$. E, consoante a definição de S, *existem* inteiros x e y tais que $d = ax + by$.

Posto isto, vamos mostrar que $d = mdc(a,b)$. Com efeito, pelo *algoritmo da divisão*, temos:

$$a = dq + r, \quad com \quad 0 \leqslant r < d$$

o que dá:

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

isto é, o *resto* r é uma *combinação linear* de a e b. Como $0 \leqslant r < d$ e $d > 0$ é o *elemento mínimo* de S, segue-se que $r = 0$ e $a = dq$, isto é, $d|a$.

Com raciocínio inteiramente análogo se conclui que também $d|b$. Logo, d é um *divisor comum positivo* de a e b.

Finalmente, se c é um *divisor comum positivo* qualquer de a e b ($c|a$ e $c|b$, $c > 0$), então:

$$c|(ax + by) \Longrightarrow c|d \Longrightarrow c \leqslant d$$

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

$$mdc(a,b) = d = ax + by, \quad x,y \in Z$$

e o teorema fica demonstrado.

NOTA. A demonstração do teorema 5.1 deixa ver que o mdc (a,b) é o *menor* inteiro positivo da forma $ax + by$, isto é, que pode ser expresso como *combinação linear* de a e b. Mas, esta *representação* do mdc(a,b) como *combinação linear* de a e b *não é única*, pois, temos:

$$mdc(a,b) = d = a(x + bt) + b(y - at)$$

qualquer que seja o inteiro t.

Importa ainda notar que, se

$$d = ar + bs$$

para algum par de inteiros r e s, então d não é necessariamente o mdc(a,b). Assim, p.ex., se:

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

então

$$t.mdc(a,b) = atx + bty$$

para todo inteiro t, isto é:

$$d = ar + bs$$

onde $d = t.mdc(a,b)$, $r = tx$ e $s = ty$.

Exemplo 5.3 Sejam os inteiros $a = 6$ e $b = 27$. Temos:

$$mdc(6,27) = 3 = \underset{x}{6(-4)} + \underset{y}{27.1}$$

e, portanto:

$$d = a(x + bt) + b(y - at)$$

$$mdc(6,27) = 3 = 6(-4 + 27t) + 27(1 - 6t)$$

qualquer que seja o inteiro t.

Exemplo 5.4 Sejam os inteiros $a = -8$ e $b = -36$. Temos:

$$mdc(-8,-36) = 4 = \underbrace{\overset{a}{(-8)}\overset{x}{4}}_{-32} + \underbrace{\overset{b}{(-36)}\overset{y}{(-1)}}_{+36}$$

Teorema 5.2 Se a e b são dois inteiros não conjuntamente nulos ($a \neq 0$ ou $b \neq 0$), então o conjunto de todos os *múltiplos* do $mdc(a,b) = d$ é

$$T = \{ax + by \mid x,y \in Z\}$$

Demonstração:

Como $d|a$ e $d|b$, segue-se que $d|(ax + by)$, quaisquer que sejam os inteiros x e y, e por conseguinte todo elemento do conjunto T é um *múltiplo* de d.

Por outro lado, existem inteiros x_o e y_o tais que

$$d = ax_o + by_o,$$

de modo que todo *múltiplo* kd de d é da forma:

$$kd = k(ax_o + by_o) = a(kx_o) + b(ky_o)$$

isto é, kd é uma *combinação linear* de a e b e, portanto, kd é elemento do conjunto T.

5.3 INTEIROS PRIMOS ENTRE SI

Definição 5.2 Sejam a e b dois inteiros não conjuntamente nulos ($a \neq 0$ ou $b \neq 0$). Diz-se que a e b são *primos entre si* se e somente se o $mdc(a,b) = 1$.

Assim, p.ex., são *primos entre si* os inteiros: 2 e 5, -9 e 16, -27 e -35, pois, temos:

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

Dois inteiros a e b *primos entre si* admitem como *únicos divisores comuns* 1 e -1.

Teorema 5.3 Dois inteiros a e b, não conjuntamente nulos ($a \neq 0$ ou $b \neq 0$), são *primos entre si* se e somente se existem inteiros x e y tais que $ax + by = 1$.

Demonstração:

($\Longrightarrow$) Se a e b são *primos entre si*, então o mdc(a,b) = = 1 e por conseguinte existem inteiros x e y tais que

$$ax + by = 1.$$

($\Longleftarrow$) Reciprocamente, se existem inteiros x e y tais que $ax + by = 1$ e se o mdc(a,b) = d, então $d|a$ e $d|b$. Logo, $d|(ax + by)$ e $d|1$, o que implica $d = 1$ ou mdc(a,b) = 1, isto é, a e b são *primos entre si*.

Corolário 5.1 Se o mdc(a,b) = d, então o mdc(a/d, b/d) = = 1.

Demonstração:

Preliminarmente, observe-se que a/d e b/d são *inteiros*, porque d é um *divisor comum* de a e b.

Posto isto, se o mdc(a,b) = d, então existem inteiros x e y tais que $ax + by = d$, ou seja, dividindo ambos os membros desta igualdade por d:

$$(a/d)x + (b/d)y = 1$$

Logo, pelo teorema anterior, os inteiros a/d e b/d são *primos entre si*, isto é, o mdc(a/d, b/d) = 1.

Assim, p.ex.:

$$\text{mdc}(-12,30) = 6 \quad \text{e} \quad \text{mdc}(-12/6,\ 30/6) = \text{mdc}(-2,5)=1$$

<u>Corolário 5.2</u> Se $a|b$ e se o $mdc(b,c) = 1$, então o $mdc(a,c) = 1$.

<u>Demonstração:</u>

Com efeito:

$$a|b \Longrightarrow b = aq, \quad \text{com} \quad q \in Z$$

$$mdc(b,c) = 1 \Longrightarrow bx + cy = 1, \text{ com } x,y \in Z$$

Portanto:

$$a(qx) + cy = 1 \Longrightarrow mdc(a,c) = 1$$

<u>Corolário 5.3</u> Se $a|c$, se $b|c$ e se o $mdc(a,b) = 1$, então $ab|c$.

<u>Demonstração:</u>

Com efeito:

$$a|c \Longrightarrow c = aq_1, \quad \text{com} \quad q_1 \in Z$$

$$b|c \Longrightarrow c = bq_2, \quad \text{com} \quad q_2 \in Z$$

$$mdc(a,b) = 1 \Longrightarrow ax + by = 1, \quad \text{com} \quad x,y \in Z$$

$$\Longrightarrow acx + bcy = c$$

Portanto:

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

Observe-se que somente as condiçoes $a|c$ e $b|c$ não implicam $ab|c$.

Assim, p.ex., $6|24$ e $8|24$, mas $6.8 \nmid 24$ (o $mdc(6,8) = 2 \neq 1$).

<u>Corolário 5.4</u> Se $mdc(a,b) = 1 = mdc(a,c)$, então $mdc(a,bc) = 1$.

<u>Demonstração:</u>

Com efeito:

$$mdc(a,b) = 1 \Longrightarrow ax + by = 1, \text{ com } x,y \in Z$$

$$mdc(a,c) = 1 \Longrightarrow az + ct = 1, \text{ com } z,t \in Z$$

Portanto:

$$1 = ax + by(az + ct) = a(x + byz) + bc(yt)$$

o que implica $mdc(a,bc) = 1$.

<u>Corolário 5.5</u> Se o $mdc(a,bc) = 1$, então $mdc(a,b) = 1 = mdc(a,c)$.

<u>Demonstração:</u>

Com efeito:

$$mdc(a,bc) = 1 \Longrightarrow ax + (bc)y = 1, \text{ com } x,y \in Z$$

Portanto:

$$ax + b(cy) = 1 \Longrightarrow mdc(a,b) = 1$$

$$ax + c(by) = 1 \Longrightarrow mdc(a,c) = 1$$

Note-se que esta proposição é a *recíproca* da anterior.

<u>Teorema 5.4</u> (de EUCLIDES) Se $a|bc$ e se o $mdc(a,b) = 1$, então $a|c$.

<u>Demonstração:</u>

Com efeito:

$$a|bc \Longrightarrow bc = aq, \quad \text{com} \quad q \in Z$$
$$mdc(a,b) = 1 \Longrightarrow ax + by = 1, \quad \text{com } x,y \in Z$$
$$\Longrightarrow acx + bcy = c$$

Portanto:

$$c = acx + aqy = a(cx + qy) \Longrightarrow a|c$$

Note-se que somente a condição $a|bc$ não implica que $a|c$. Assim, p.ex., $12|9.8$, mas $12 \nmid 9$ e $12 \nmid 8$ $mdc(12,9) \neq 1$ e $mdc(12,8) \neq 1$).

5.4 CARACTERIZAÇÃO DO MDC DE DOIS INTEIROS

<u>Teorema 5.5</u> Sejam <u>a</u> e <u>b</u> dois inteiros não conjuntamente nulos ($a \neq 0$ ou $b \neq 0$). Um inteiro *poditivo* <u>d</u> ($d > 0$) é o $mdc(a,b)$ se e somente se satisfaz às condições:

(1) $d|a$ e $d|b$

(2) se $c|a$ e se $c|b$, então $c|d$

Demonstração:

($\Longrightarrow$) Suponhamos que o mdc(a,b) = d. Então, $d|a$ e $d|b$, isto é, a condição (1) é satisfeita. Por outra parte, existem inteiros x e y tais que $ax + by = d$ e, portanto, se $c|a$ e se $c|b$, então $c|(ax + by)$ e $c|d$, isto é, a condição (2) também é satisfeita.

($\Longrightarrow$) Reciprocamente, seja d um inteiro positivo qualquer que satisfaz às condições (1) e (2). Então, pela condição (2), todo divisor comum c de a e b também é divisor de d, isto é, $c|d$, e isto implica $c \leq d$. Logo, d é o mdc(a,b).

5.5 MDC DE VÁRIOS INTEIROS

O conceito de *máximo divisor comum*, definido para dois inteiros a e b, estende-se de maneira natural a mais de dois inteiros. No caso de três inteiros a, b e c, não todos nulos, o mdc(a,b,c) é o inteiro *positivo* d ($d > 0$) que satisfaz às condições:

(1) $d|a$, $d|b$ e $d|c$

(2) se $e|a$, se $e|b$ e se $e|c$, então $e \leq d$

Assim, p.ex.:

$$\text{mdc}(39,42,54) = 3 \quad \text{e} \quad \text{mdc}(49,210,350) = 7$$

Importa notar que três inteiros a, b e c podem ser *primos entre si*, isto é, o mdc(a,b,c) = 1, sem que sejam *primos entre si dois a dois*, que é o caso, p.ex., dos inteiros 6, 10 e 15.

Teorema 5.6 O mdc(a,b,c) = mdc(mdc(a,b),c).

Demonstração:

Com efeito, seja mdc(a,b,c) = d e mdc(a,b) = e. Então, $d|a$, $d|b$ e $d|c$, e como existem inteiros x e y tais que $ax + by = e$, segue-se que $d|(ax + by)$ ou $d|e$, isto é, d é um *divisor comum* de e e c ($d|e$ e $d|c$).

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

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

Exemplo 5.5 Determinar o mdc(570, 810, 495).

Pelo teorema anterior, temos:

$$\text{mdc}(570,810,495) = \text{mdc}(\text{mdc}(570,810),495)$$

e como o mdc(570,810) = 30, segue-se que o

$$\text{mdc}(570,810,495) = \text{mdc}(30,495) = 15$$

EXERCÍCIOS

1. Determinar:

   (a) mdc(11, 99)

   (b) mdc(-21,14) (c) mdc(17,18)

2. Achar os elementos do conjunto {1,2,3,4,5} que são *primos* com 8.

3. Seja o conjunto A = {1,2,3,4,5,6}. Enumerar os elementos do conjunto:

$$X = \{x \in A \mid \text{mdc}(x,6) = 1\}$$

4. Sabendo que o mdc(a,0) = 13, achar os valores do inteiro a.

5. Achar o *menor* inteiro positivo c da forma

$$c = 22x + 55y,$$

   onde x e y são dois inteiros.

6. Sendo n um inteiro qualquer, calcular o mdc(n, n+1).

7. Calcular:

   (a) mdc(n, n+2), sendo n um inteiro *par;*

   (b) mdc(n, n+2), sendo n um inteiro *ímpar.*

8. Sendo $\underline{n}$ um inteiro qualquer, achar os possíveis valores do máximo divisor comum dos inteiros $\underline{n}$ e $\underline{n+10}$.

9. Sendo $\underline{n}$ um inteiro qualquer, calcular o

$$mdc(n-1,\ n^2 + n + 1).$$

10. Sendo $\underline{a}$ e $\underline{b}$ dois inteiros não conjuntamente nulos ($a \neq 0$ ou $b \neq 0$), mostrar:

$$mdc(a,b) = mdc(-a,b) = mdc(a,-b) = mdc(-a,-b)$$

11. Sejam $\underline{a}$, $\underline{b}$ e $\underline{c}$ inteiros. Demonstrar:

(a) existem inteiros $\underline{x}$ e $\underline{y}$ tais que $c = ax + by$ se e somente se o $mdc(a,b) | c$;

(b) se existem inteiros $\underline{x}$ e $\underline{y}$ tais que $ax+by=mdc(a,b)$, então o $mdc(x,y) = 1$.

12. Sejam $\underline{a}$, $\underline{b}$ e $\underline{c}$ inteiros. Demonstrar:

(a) Se o $mdc(a,b) = 1$, então o $mdc(ac,b) = mdc(b,c)$.

(b) Se o $mdc(a,b) = 1$ e se $c | (a+b)$, então o $mdc(a,c) = 1$ e o $mdc(b,c) = 1$.

(c) Se $b | c$, então o $mdc(a,b) = mdc(a + c,\ b)$.

(d) Se o $mdc(a,b) = 1$, então o $mdc(a^m,b^n) = 1$, onde $\underline{m}$ e $\underline{n}$ são inteiros positivos.

13. Calcular o $mdc(a+b,\ a-b)$, sabendo que $\underline{a}$ e $\underline{b}$ são inteiros *primos entre si*.

14. O mdc de dois inteiros positivos é 10 e o *maior* déles é 120. Determinar o outro inteiro.

15. Achar o *maior* inteiro positivo pelo qual se devem dividir os inteiros 160, 198 e 370 para que os *restos* sejam respectivamente 7, 11 e 13.

16. Determinar os inteiros positivos a e b sabendo:

    (a) $a + b = 63$ e o $mdc(a,b) = 9$

    (b) $ab = 756$ e o $mdc(a,b) = 6$

17. Os *restos* das divisões dos inteiros 4933 e 4435 por um inteiro positivo n são respectivamente 37 e 19. Achar o inteiro n.

18. Demonstrar que, se $n = abc + 1$, então o $mdc(n,a) = mdc(n,b) = mdc(n,c) = 1$.

19. Demonstrar que o $mdc(mdc(a,b),b) = mdc(a,b)$.

20. Demonstrar que o $mdc(n + k,k) = 1$ se e somente se o $mdc(n,k) = 1$.

21. Demonstrar que, se $a|bc$ e se o $mdc(a,b) = d$, então $a|cd$.

22. Demonstrar que, se $a|c$, se $b|c$ e se o $mdc(a,b) = d$, então $ab|cd$.

23. Demonstrar que, se o $mdc(a,b) = 1$ e se o $mdc(a,c) = d$, então $mdc(a,bc) = d$.

24. O inteiro ímpar $\underline{d}$ é um *divisor* de $a+b$ e de $a-b$. Demonstrar que $\underline{d}$ também é um *divisor* do $mdc(a,b)$.

25. Os inteiros positivos $\underline{a}$, $\underline{b}$ e $\underline{c}$ são tais que o $mdc(a,b) = 1$, $a|c$ e $c|b$. Demonstrar que $a = 1$.

26. O $mdc(n,n + k) = 1$ para todo inteiro positivo $\underline{n}$. Demonstrar que $k = 1$ ou $k = -1$.

27. Demonstrar que o $mdc(a,b) = mdc(a + kb,b)$ para todo inteiro $\underline{k}$.

28. O $mdc(a,4) = 2 = mdc(b,4)$. Demonstrar que o $mdc(a + b,4) = 4$.

29. Os inteiros positivos $\underline{m}$ e $\underline{n}$ são tais que o $mdc(m,n) = d$. Mostrar que o $mdc(2^m - 1, 2^n - 1) = 2^d - 1$.

30. Demonstrar que o $mdc(a,b) = mdc(a,b,a + b)$.

31. Demonstrar que o $mdc(a,b) = mdc(a,b,ax + by)$, quaisquer que sejam os inteiros $\underline{x}$ e $\underline{y}$.

32. O $mdc(a,b) = p$, sendo $\underline{p}$ um *primo*. Achar os possíveis valores do:

(a) $mdc(a^2,b)$:

(b) $mdc(a^3,b)$; (c) $mdc(a^2,b^3)$.

33. Sabendo que o $mdc(a,p^2) = p$ e que o $mdc(b,p^3) = p^2$, onde $\underline{p}$ é um primo, calcular o $mdc(ab,p^4)$ e o $mdc(a + b,p^4)$.

34. Demonstrar que, se o $mdc(a,b) = d$, então o

$$mdc(a^2,b^2) = d^2.$$

35. Sejam a e k inteiros não conjuntamente nulos. Demonstrar que o $mdc(a, a+k) | k$.

36. Demonstrar que $mdc(a,b) = mdc(a,c)$ implica $mdc(a^2,b^2) = mdc(a^2,c^2)$.

37. Demonstrar que $mdc(a,b) = mdc(a,c)$ implica $mdc(a,b) = mdc(a,b,c)$.

38. Demonstrar que $mdc(a,b,c) = mdc(mdc(a,b),mdc(a,c))$.

39. Sejam a e b inteiros positivos tais que ab é um quadrado perfeito e o $mdc(a,b) = 1$. Demonstrar que a e b são quadrados perfeitos.

40. Demonstrar que o $mdc(a+b, a-b) \geq mdc(a,b)$.

41. Mostrar que o $mdc(5n+6, 5n+8) = 1$, onde n é um inteiro *ímpar*.

42. Sejam a, b, c, d($b \neq d$) inteiros tais que o $mdc(a,b) = mdc(c,d) = 1$. Mostrar que a soma $a/b + c/d$ não é um inteiro.

43. Determinar os inteiros positivos a e b, sabendo:

$$a^2 - b^2 = 7344 \quad e \quad mdc(a,b) = 12.$$

44. Dividindo-se dois inteiros positivos pelo seu mdc, a soma dos quocientes obtidos é 8. Determinar os dois inteiros, sabendo que a sua soma é 384.

CAPÍTULO 6

ALGORÍTMO DE EUCLIDES MÍNIMO MÚLTIPLO COMUM

<u>Lema 6.1</u> Se $a = bq + r$, então o $mdc(a,b) = mdc(b,r)$.

<u>Demonstração</u>:

Se o $mdc(a,b) = d$, então $d|a$ e $d|b$, o que implica $d|(a - bq)$ ou $d|r$, isto é, $\underline{d}$ é um *divisor comum* de $\underline{b}$ e $\underline{r}$ ($d|b$ e $d|r$).

Por outro lado, se $\underline{c}$ é um *divisor comum* qualquer de $\underline{b}$ e $\underline{r}$ ($c|b$ e $c|r$), então $c|(bq + r)$ ou $c|a$, isto é, $\underline{c}$ é um *divisor comum* de $\underline{a}$ e $\underline{b}$, o que implica $c \leqslant d$. Assim sendo, o $mdc(b,r) = d$.

6.1 ALGORITMO DE EUCLIDES

Sejam $\underline{a}$ e $\underline{b}$ dois inteiros não conjuntamente nulos ($a \neq 0$ ou $b \neq 0$) cujo *máximo divisor comum* se deseja determinar.

É imediato:

(1) se $a \neq 0$, então o $mdc(a,0) = |a|$

(2) se $a \neq 0$, então o $mdc(a,a) = |a|$

(3) se $b|a$, então o $mdc(a,b) = |b|$

Além disso, por ser $mdc(a,b) = mdc(|a|, |b|)$, a determinação do $mdc(a,b)$ reduz-se ao caso em que $\underline{a}$ e $\underline{b}$ são inteiros positivos *distintos*, p.ex., com $a > b$, tais que $\underline{b}$ *não divide* $\underline{a}$, isto é: $a > b > 0$ e $b \nmid a$. Nestas condições, a aplicação repetida do *algoritmo da divisão* dá-nos as igualdades:

$$a = bq_1 + r_1 , \quad 0 < r_1 < b$$

$$b = r_1q_2 + r_2 , \quad 0 < r_2 < r_1$$

$$r_1 = r_2q_3 + r_3, \quad 0 < r_3 < r_2$$

$$r_2 = r_3q_4 + r_4, \quad 0 < r_4 < r_3$$

$$\ldots\ldots\ldots\ldots\ldots \quad \ldots\ldots\ldots$$

Como os *restos* $r_1, r_2, r_3, r_4, \ldots$ são todos inteiros positivos tais que

$$b > r_1 > r_2 > r_3 > r_4 > \ldots$$

e existem apenas $b-1$ inteiros positivos menores que $\underline{b}$, necessariamente se chega a uma divisão cujo resto $r_{n+1} = 0$, isto é, finalmente, teremos:

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

$$r_{n-1} = r_nq_{n+1} + r_{n+1} , \quad r_{n+1} = 0$$

O último resto $r_n \neq 0$ que aparece nesta sequência de divisões é o *máximo divisor comum* procurado de a e b, isto é, o $mdc(a,b) = r_n$, visto que, pelo lema anterior, temos:

$$mdc(a,b) = mdc(b,r_1) = mdc(r_1,r_2) = \dots =$$
$$= mdc(r_{n-2},r_{n-1}) = mdc(r_{n-1},r_n) = r_n$$

Este processo prático para o cálculo do *máximo divisor comum* de dois inteiros positivos a e b é denominado *algoritmo de EUCLIDES* ou *processo das divisões sucessivas*.

É usual o seguinte dispositivo de cálculo no emprego do *algoritmo de EUCLIDES:*

	q_1	q_2	q_3		q_n	q_{n+1}
a	b	r_1	r_2	...	r_{n-1}	r_n
r_1	r_2	r_3	r_4		0	

que se traduz na seguinte *REGRA*: Para se "*achar*" o mdc de dois inteiros positivos, divide-se o maior pelo menor, este pelo primeiro resto obtido, o segundo resto pelo primeiro, e assim sucessivamente até se encontrar um *resto nulo*. O último *resto não nulo* é o *máximo divisor comum procurado*.

O *algoritmo de EUCLIDES* também ser usado para achar a expressão do $mdc(a,b) = r_n$ como *combinação linear* de a e b, para o que basta eliminar sucessivamente os restos r_{n-1},

$r_{n-2},\ldots,r_3,r_2,r_1$ entre as n primeiras igualdades anteriores.

Exemplo 6.1 Achar o mdc(963,657) pelo *algoritmo de EUCLIDES* e a sua expressão como *combinação linear de* 963 e 657.

Temos, sucessivamente:

963 = 657.1 + 306
657 = 306.2 + 45
306 = 45.6 + 36
45 = 36.1 + 9
36 = 9.4 + 0

	1	2	6	1	4
963	657	306	45	36	9
306	45	36	9	0	

Portanto, o mdc(963,657) = 9 e a sua expressão como *combinação linear de* 963 e 657 se obtém eliminando os *restos* 36, 45 e 306 entre as quatro primeiras igualdades anteriores do seguinte modo:

$$9 = 45 - 36 = 45 - (306 - 45.6) =$$
$$= -306 + 7.45 = -306 + 7(657 - 306.2) =$$
$$= 7.657 - 15.306 = 7.657 - 15(963 - 657) =$$
$$= 963(-15) + 657.2$$

isto é:

$$9 = \text{mdc}(963,657) = 963x + 657y$$

onde $x = -15$ e $y = 22$.

Esta *representação* do inteiro 9 = mdc(963,657) como *combinação linear de* 963 *e* 657 *não é única*. Assim, p.ex.,somando e subtraindo o produto 963.657 ao segundo membro da igualdade:

$$9 = 963(-15) + 657.22$$

obtemos:

$$9 = 963(-15 + 657) + 657(22 - 963) =$$

$$= 963.642 + 657(-941)$$

que é uma outra *representação* do inteiro 9 = mdc(963,657) como *combinação linear de* 963 *e* 657.

<u>Exemplo 6.2</u> Achar o mdc(252,-180) pelo *algoritmo de EUCLIDES* e a sua expressão como *combinação linear de* 252 *e* -180.

Temos, sucessivamente:

$$252 = 180.1 + 72$$

$$180 = 72.2 + 36$$

$$72 = 36.2$$

Portanto, o mdc(252,-180) = mdc(252,180) = 35, e como

$$36 = 180 - 72.2 = 180 - (252 - 180)2 =$$

$$= 252(-2) + (-180)(-3)$$

temos:

$$36 = \text{mdc}(252,-180) = 252x + (-180)y$$

onde $x = -2$ é $y = -3$, que é a expressão do mdc(252, -180) como *combinação linear de* 252 *e* -180.

Outra *representação* do inteiro $36 = \text{mdc}(252,-180)$ como *combinação linear de* 252 *e* -180 é a seguinte:

$$36 = 252(-2 + 180) + (-180)(-3 + 252) =$$

$$= 252.178 + (-180)249$$

<u>Exemplo 6.3</u> O <u>mdc</u> de dois inteiros positivos <u>a</u> e <u>b</u> é 74 e na sua determinação pelo *algoritmo de EUCLIDES* os quocientes obtidos foram 1, 2, 2, 5, 1 e 3. Calcular <u>a</u> e <u>b</u>.

	1	2	2	5	1	3
a	b	r	r_1	r_2	r_3	74
r	r_1	r_2	r_3	74	0	

Temos, sucessivamente:

$$a = b + r, \quad b = 2r + r_1, \quad r = 2r_1 + r_2$$

$$r_1 = 5r_2 + r_3, \quad r_2 = r_3 + 74, \quad r_3 = 74.3 = 222$$

Portanto:

$$r_2 = 222 + 74 = 296, \quad r_1 = 5.296 + 222 = 1702$$

$$r = 2.1702 + 296 = 3700, \quad b = 2.3700 + 1702 = 9102$$

$$a = 9102 + 3700 = 12802$$

Teorema 6.1 Se $k > 0$, então o $mdc(ka, kb) = k.mdc(a,b)$.

Demonstração:

Multiplicando ambos os membros de cada uma das n+1 igualdades que dão o $mdc(a,b) = r_n$ pelo *algoritmo de EUCLIDES* por k, obtemos:

$$
\begin{aligned}
ak &= (bk)q_1 + r_1k, & 0 < r_1k < bk \\
bk &= (r_1k)q_2 + r_2k, & 0 < r_2k < r_1k \\
r_1k &= (r_2k)q_3 + r_3k, & 0 < r_3k < r_2k \\
&\cdots\cdots\cdots\cdots & \cdots\cdots\cdots \\
r_{n-2}k &= (r_{n-1}k)q_n + r_nk, & 0 < r_nk < r_{n-1}k \\
r_{n-1}k &= (r_nk)q_{n+1} + 0
\end{aligned}
$$

Obviamente, estas n+1 igualdades outra coisa não são que o *algoritmo de EUCLIDES* aplicado aos inteiros ak e bk, e por conseguinte o $mdc(ak, bk)$ é o último *resto* $r_nk \neq 0$, isto é:

$$mdc(ak, bk) = r_nk = k.mdc(a,b)$$

Assim, p.ex.:

$$mdc(12,30) = mdc(2.6, 5.6) = 6.mdc(2,5) = 6.1 = 6$$

Corolário 6.1 Para todo $k \neq 0$, o $mdc(ka,kb) = |k| . mdc(a,b)$.

Demonstração:

Se $k > 0$, nada há que demonstrar, e se $k < 0$, então $-k = |k| > 0$ e, pelo teorema anterior, temos:

$$\text{mdc}(ak, bk) = \text{mdc}(-ak, -bk) =$$

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

6.2 MÚLTIPLOS COMUNS DE DOIS INTEIROS

O conjunto de todos os *múltiplos* de um inteiro qualquer $a \neq 0$ indica-se por $M(a)$, isto é:

$$M(a) = \{ x \in Z \ \ |a|x \} = \{ aq \mid q \in Z \}$$

Assim, p.ex.:

$$M(-1) = M(1) = Z$$

$$M(5) = \{ 5q \mid q \in Z \} = \{ 0, \pm 5, \pm 10, \pm 15, \pm 20, \ldots \}$$

É imediato que, para todo inteiro $a \neq 0$, se tem $M(a) = M(-a)$.

Definição 6.1 Sejam a e b dois inteiros diferentes de zero ($a \neq 0$ e $b \neq 0$). Chama-se *múltiplo comum* de a e b todo inteiro x tal que $a|x$ e $b|x$.

Em outros termos, *múltiplo comum* de a e b é todo inteiro que pertence simultaneamente aos conjuntos $M(a)$ e $M(b)$.

O conjunto de todos os *múltiplos comuns* de $\underline{a}$ e de $\underline{b}$ indica se por M(a,b). Portanto, simbolicamente:

$$M(a,b) = \{ x \in Z \quad |a|x \quad e \quad b|x \}$$

ou seja:

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

e, portanto:

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

A *interseção* ($\cap$) é uma *operação comutativa*, de modo que M(a,b) não depende da *ordem* dos inteiros dados $\underline{a}$ e $\underline{b}$, isto é: $M(a,b) = M(b,a)$.

Obviamente, 0 é um *múltiplo comum* de $\underline{a}$ e $\underline{b}$: $0 \in M(a,b)$. E os produtos $\underline{ab}$ e $-(\underline{ab})$ também são *múltiplos comuns* de $\underline{a}$ e $\underline{b}$.

<u>Exemplo 6.4</u> Sejam os inteiros $a = 12$ e $b = -18$. Temos:

$$M(12) = \{ 12q \mid q \in Z \} = \{ 0, \pm 12, \pm 24, \pm 36, \pm 48, \pm 60, \pm 72, \ldots \}$$

$$M(-18) = \{ -18q \mid q \in Z \} = \{ 0, \pm 18, \pm 36, \pm 54, \pm 72, \pm 90, \ldots \}$$

Portanto:

$$M(12,-18) = M(12) \cap M(-18) = \{ 0, \pm 36, \pm 72, \ldots \}$$

6.3 MÍNIMO MÚLTIPLO COMUM DE DOIS INTEIROS

Definição 6.2 Sejam a e b dois inteiros diferentes de zero ($a \neq 0$ e $b \neq 0$). Chama-se *mínimo múltiplo comum* de a e b o inteiro positivo m ($m > 0$) que satisfaz às condições:

(1) $a|m$ e $b|m$

(2) se $a|c$ e se $b|c$, com $c > 0$, então $m \leq c$.

Observe-se que, pela condição (1), m é um múltiplo comum de a e b, e pela condição (2), m é o *menor* dentre todos os múltiplos comuns *positivos* de a e b.

O *mínimo múltiplo comum* de a e b indica-se pela notação mmc(a,b).

Pelo *"Princípio da boa ordenação"*, o conjunto dos múltiplos comuns positivos de a e b possui o *elemento mínimo* e, portanto, o mmc(a,b) *existe* sempre e é *único*. Além disso, por ser o produto ab um *múltiplo comum* de a e b, segue-se que o $\text{mmc}(a,b) \leq |ab|$.

Em particular, se $a|b$, então o $\text{mmc}(a,b) = |b|$.

Exemplo 6.5 Sejam os inteiros $a = -12$ e $b = 30$. Os múltiplos comuns *positivos* de -12 e 30 são $60, 120, 180, \ldots$, e como o *menor* deles é 60, segue-se que o $\text{mmc}(-12,30) = 60$.

6.4 RELAÇÃO ENTRE O MDC E O MMC

Teorema 6.2 Para todo par de inteiros positivos a e b subsiste a relação:

$$mdc(a,b).mmc(a,b) = ab$$

Demonstração:

Seja $mdc(a,b) = d$ e $mmc(a,b) = m$. Como $a|a(b/d)$ e $b|b(a/d)$, segue-se que ab/d é um *múltiplo comum* de a e b. Portanto, existe um inteiro positivo k tal que

$$ab/d = mk, \quad k \in N$$

o que implica:

$$a/d = (m/b)k \quad e \quad b/d = (m/a)k$$

isto é, k é um *divisor comum* dos inteiros a/d e b/d. Mas, a/d e b/d são *primos entre si* (Corolário 5.1), de modo que k = 1. Assim sendo, temos:

$$ab/d = m \quad ou \quad ab = dm$$

isto é:

$$ab = mdc(a,b).mmc(a,b)$$

Esta importante relação permite determinar o mmc de dois inteiros quando se conhece o seu mdc, e vice-versa.

Exemplo 6.6 Determinar o mmc(963, 657).

Pelo algoritmo de EUCLIDES, temos mdc(963, 657) = 9. Portanto:

$$\text{mmc}(963,\ 657) = \frac{963.657}{9} = 70299$$

Corolário 6.2 Para todo par de inteiros positivos a e b, o mmc(a,b) = ab se e somente se o mdc(a,b) = 1.

Demonstração:

($\Longrightarrow$) Se o mdc(a,b) = 1, então:

$$ab = 1.\text{mmc}(a,b) = \text{mmc}(a,b)$$

($\Longrightarrow$) Reciprocamente, se o mmc(a,b) = ab, então:

$$\text{mdc}(a,b).ab = ab \Longrightarrow \text{mdc}(a,b) = 1$$

6.5 MMC DE VÁRIOS INTEIROS

O conceito de *mínimo múltiplo comum*, definido para dois inteiros a e b, estende-se de maneira natural a mais de dois inteiros. No caso de três inteiros a, b, e c, diferentes de zero, o mmc(a,b,c) é o inteiro *positivo* m ($m > 0$) que satisfaz às condições:

(1) $a|m$, $b|m$ e $c|m$

(2) se $a|e$, se $b|e$ e se $c|e$, com $e > 0$, então $m \leq e$.

Assim, p.ex.: mmc(39, 102, 75) = 33150

EXERCÍCIOS

1. Usando o *algoritmo de EUCLIDES*, determinar:

   (a) mdc(306, 657) (b) mdc(272, 1479)

   (c) mdc(884,1292) (d) mdc(-816, 7209)

   (e) mdc(7469, 2387) (f) mdc(-5376, -3402)

2. Usando o *algoritmo de EUCLIDES*, determinar:

   (a) mdc(624, 504, 90) (b) mdc(285, 675, 405)

   (c) mdc(209, 299, 102) (d) mdc(69, 598, 253)

3. Usando o *algoritmo de EUCLIDES*, achar inteiros $\underline{x}$ e $\underline{y}$ que verifiquem cada uma das seguintes igualdades:

   (a) $\text{mdc}(56, 72) = 56x + 72y$

   (b) $\text{mdc}(24, 138) = 24x + 138y$

   (c) $\text{mdc}(119, 272) = 119x + 272y$

   (d) $\text{mdc}(1769, 2378) = 1769x + 2378y$

4. Achar inteiros $\underline{x}$ e $\underline{y}$ que verifiquem cada uma das seguintes igualdades:

   (a) $78x + 32y = 2$ (b) $104x + 91y = 13$

   (c) $31x + 19y = 7$ (d) $42x + 26y = 16$

   (e) $238x + 51y = 3$ (f) $52x + 13y = 1$

   (g) $145x + 58y = 87$ (h) $17x + 5y = -2$

5. Achar inteiros x, y e z que verifiquem cada uma das seguintes igualdades:

(a) $11x + 19y + 3z = 1$ (b) $56x + 6y + 32z = 2$

(c) $6x + 3y + 15z = 9$ (d) $14x + 7y + 21z = 4$

6. Achar inteiros x, y e z que verifiquem a igualdade:

$$198x + 288y + 512z = \text{mdc}(198, 288, 512)$$

7. Calcular:

(a) mmc(45, 21)

(b) mmc(83, 68)

(c) mmc(120, 110)

(d) mmc(86, 71)

(e) mmc(224, 192)

(f) mmc(1287, 507)

(g) mmc(143, 227)

(h) mmc(306, 657)

8. O mdc de dois inteiros positivos a e b é 8 e na sua determinação pelo *algoritmo de EUCLIDES* os quocientes sucessivamente obtidos foram 2, 1, 1 e 4. Calcular a e b.

9. Determinar os inteiros positivos a e b sabendo:

(a) $ab = 4032$ e o $\text{mmc}(a,b) = 336$

(b) $\text{mdc}(a,b) = 8$ e o $\text{mmc}(a,b) = 560$

(c) $a + b = 589$ e $\dfrac{\text{mmc}(a,b)}{\text{mdc}(a,b)} = 84$.

10. Demonstrar que, se a e b são inteiros positivos tais que o mdc(a,b) = mmc(a,b), então a = b.

11. Sabendo que o mdc(a,b) = 1, demonstrar:

(a) mdc(2a+ b, a + 2b) = 1 ou 3

(b) mdc(a + b, $a^2 + b^2$) = 1 ou 2

(c) mdc(a + b, $a^2 - ab + b^2$) = 1 ou 3

12. Sendo a e b inteiros positivos, demonstrar que o mdc(a,b) sempre *divide* o mmc(a,b).

CAPÍTULO 7

NÚMEROS PRIMOS

7.1 NÚMEROS PRIMOS E COMPOSTOS

Definição 7.1 Diz-se que um inteiro positivo $p > 1$ é um *número primo* ou apenas um *primo* se e somente se 1 e p são os seus únicos divisores positivos. Um inteiro positivo maior que 1 e que não é primo diz-se *composto*.

Assim, p.ex., os inteiros positivos 2, 3, 5 e 7 são todos *primos* e os inteiros positivos 4,6,8 e 10 são todos *compostos*.

O inteiro positivo 1 não é nem primo nem composto, e por conseguinte se a é um inteiro positivo qualquer, então a é *primo*, ou a é *composto* ou $a = 1$.

Observe-se que 2 é o único inteiro positivo par que é *primo*.

Teorema 7.1 Se um *primo* p não divide um inteiro a, então a e p são *primos entre si*.

Demonstração:

Seja d o mdc de a e p. Então $d|a$ e $d|p$. Da relação $d|p$, resulta que $d = 1$ ou $d = p$, porque p é *primo*, e como a segunda igualdade é impossível, porque p não divide a, segue-se que $d = 1$, isto é, o $mdc(a,p) = 1$. Logo, a e p são *primos entre si*.

Corolário 7.1 Se p é um *primo* tal que $p|ab$, então $p|a$ ou $p|b$.

Demonstração:

Se $p|a$, nada há que demonstrar, e se, ao invés, p não divide a, então, pelo teorema anterior, o $mdc(p,a) = 1$. Logo, pelo teorema 5.4 (de EUCLIDES), $p|b$.

Corolário 7.2 Se p é um *primo* tal que $p|a_1a_2\ldots a_n$, então existe um índice k, com $1 \leqslant k \leqslant n$, tal que $p|a_k$.

Demonstração:

Usando o "Teorema da indução matemática", a proposição é verdadeira p/ $n=1$ (imediato) e para $n = 2$ (pelo Corolário 7.1). Suponhamos, pois, $n > 2$ e que, se p divide um produto com menos de n fatores, então p divide pelo menos um dos fatores (*hipótese de indução*).

Pelo corolário 7.1, se $p|a_1a_2\ldots a_n$, então

$$p|a_n \quad \text{ou} \quad p|a_1a_2\ldots a_{n-1}$$

Se $p|a_n$, a proposição está demonstrada, e se, ao invés, $p|a_1a_2\ldots a_{n-1}$, então a *hipótese de indução* assegura que $p|a_k$, com $1 \leqslant k \leqslant n-1$, Em qualquer dos dois casos, p divide um dos inteiros $a_1, a_2, \ldots, a_n$.

Corolário 7.3 Se os inteiros $p, q_1, q_2, \ldots, q_n$ são todos *primos* e se $p|q_1q_2\ldots q_n$, então existe um índice k, com $1 \leqslant k \leqslant n$, tal que $p = a_k$.

Demonstração:

Com efeito, pelo corolário 7.2, existe um índice k, com $1 \leqslant k \leqslant n$, tal que $p|q_k$, e como os únicos divisores positivos de q_k são 1 e q_k, porque q_k é *primo*, segue-se que $p = 1$ ou $p = q_k$. Mas, $p > 1$, porque p é *primo*. Logo, $p = q_k$.

Teorema 7.2 Todo inteiro *composto* possui um *divisor primo*.

Demonstração:

Seja a um inteiro *composto*. Consideremos o conjunto A de todos os *divisores positivos* de a, exceto os *divisores triviais* 1 e a, isto é:

$$A = \{ x|a \mid 1 < x < a \}$$

Pelo "*Princípio da boa ordenação*" existe o *elemento mínimo* p de A, que vamos mostrar ser *primo*. Com efeito, se p fos-

se *composto* admitiria pelo menos um divisor d tal que $1 < d < p$, e então $d|p$ e $p|a$, o que implica $d|a$, isto é, p não seria o *elemento mínimo* de A. Logo, p é *primo*.

7.2 TEOREMA FUNDAMENTAL DA ARITMÉTICA

Todo inteiro positivo $n > 1$ é igual a um produto de fatores *primos*.

Demonstração:

Com efeito, se n é primo, nada há que demonstrar, e se n é *composto*, então, pelo teorema 7.2, possui um *divisor primo* p_1, e temos:

$$n = p_1 n_1, \quad 1 < n_1 < n$$

Se n_1 é *primo*, então esta igualdade representa n como produto de fatores primos, e se, ao invés, n_1 é *composto*, então, pelo teorema 7.2, possui um *divisor primo* p_2, isto é, $n_1 = p_2 n_2$, e temos:

$$n = p_1 p_2 n_2, \quad 1 < n_2 < n_1$$

Se n_2 é *primo*, então esta igualdade representa n como produto de fatores primos, e se, ao invés, n_2 é *composto*, então, pelo mesmo teorema 7.2, possui um *divisor primo* p_3, isto é, $n_2 = p_3 n_3$, e temos:

$$n = p_1 p_2 p_3 n_3, \qquad 1 < n_3 < n_2$$

e assim por diante.

Assim sendo, temos a sequência decrescente:

$$n > n_1 > n_2 > n_3 \ldots > 1$$

e como só existe um número *finito* de inteiros positivos menores que n e maiores que 1, existe necessariamente um n_k que é um *primo* p_k ($n_k = p_k$), e por conseguinte teremos:

$$n = p_1 p_2 p_3 \cdots p_k$$

igualdade que representa o inteiro positivo $n > 1$ como produto de fatores *primos*.

Corolário 7.4 A *decomposição* de um inteiro positivo $n > 1$ como produto de fatores *primos* é *única*, a menos da *ordem* dos fatores.

Demonstração:

Suponhamos que n admite *duas decomposições* como produto de fatores primos, isto é:

$$n = p_1 p_2 p_3 \cdots p_r = q_1 q_2 q_3 \cdots q_s, \qquad r \leqslant s$$

onde os p_i e os q_j são todos inteiros *primos* e tais que

$$p_1 \leqslant p_2 \leqslant p_3 \leqslant \ldots \leqslant p_r, \qquad q_1 \leqslant q_2 \leqslant q_3 \leqslant \ldots \leqslant q_s$$

Como $p_1 | q_1 q_2 q_3 \ldots q_s$, existe um índice $\underline{k}$, com $1 \leqslant k \leqslant s$, tal que $p_1 = q_k$ (Corolário 7.3), de modo que $p_1 \geqslant q_1$. Analogamente, $q_1 = p_h$, com $1 \leqslant h \leqslant r$, de modo que $q_1 \geqslant p_1$. Portanto, temos $p_1 = q_1$, o que implica:

$$p_2 p_3 \ldots p_r = q_2 q_3 \ldots q_s$$

Com o mesmo raciocínio conclui-se que $p_2 = q_2$, o que implica:

$$p_3 p_4 \ldots p_r = q_3 q_4 \ldots q_s$$

e assim por diante.

Assim sendo, se subsiste a desigualdade $r < s$, então se chega necessariamente a igualdade:

$$1 = q_{r+1} q_{r+2} \ldots q_s$$

o que é *absurdo*, porque cada $q_j > 1$. Logo, $r = s$ e temos:

$$p_1 = q_1, \quad p_2 = q_2, \ldots, \quad p_r = q_r$$

isto é, as *duas decomposições* do inteiro positivo $n > 1$ como produto de fatores primos são *idênticas*, ou seja, $\underline{n}$ admite uma *única decomposição* como produto de fatores primos.

Exemplo 7.1 A decomposição do inteiro positivo $n = 360$ num produto de fatores primos é dada pela igualdade:

$$360 = 2.2.2.3.3.5$$

Observe-se que os fatores primos 2 e 3 aparecem *repetidos*, o primeiro *três* vezes e o segundo *duas* vezes.

Corolário 7.5 Todo inteiro positivo $m > 1$ admite uma *única* decomposição da forma:

$$n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$$

onde, para $i = 1,2,\ldots,r$, cada k_i é um inteiro positivo e cada p_i é um *primo*, com $p_1 < p_2 < \ldots < p_r$, denominada *decomposição canônica* do inteiro positivo $n > 1$.

Exemplo 7.2 A *decomposição canônica* do inteiro positivo $n = 17460$ é dada pela igualdade:

$$17460 = 2^3.3^2.5.7^2$$

NOTA. Conhecidas as *decomposições canônicas* de dois inteiros positivos $a > 1$ e $b > 1$, o mdc(a,b) é o produto dos fatores primos *comuns* às duas *decomposições canônicas* tomados cada um com o *menor* expoente, e o mmc(a,b) é o produto dos fatores primos *comuns* e *não comuns* às duas *decomposições canônicas* tomados cada um com o *maior* expoente.

Assim, p.ex., as *decomposições canônicas* dos inteiros positivos 588 e 936 são:

$$588 = 2^2.3.7^2, \quad 936 = 2^3.3^2.13$$

e, portanto:

$$\text{mdc}(588, 936) = 2^2.3 = 12$$

$$\text{mmc}(588, 936) = 2^3.3^2.7^2.13 = 45864$$

Teorema 7.3 (de EUCLIDES) Há um número infinito de *primos*.

Demonstração:

Suponhamos que existe um primo p_n *maior* que todos os demais primos $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7, \ldots$, e consideremos o inteiro positivo:

$$P = p_1 p_2 p_3 \cdots p_n + 1$$

Como $P > 1$, o *"Teorema fundamental da Aritmética"* permite afirmar que P tem pelo menos um *divisor primo* p. Mas, p_1, $p_2, p_3, \ldots, p_n$ são os únicos primos, de modo que p deve, necessariamente, ser igual a um desses n primos. Assim sendo:

$$p|P \quad \text{e} \quad p|p_1 p_2 p_3 \cdots p_n$$

o que implica:

$$p|P - p_1 p_2 p_3 \cdots p_n \quad \text{ou} \quad p|1$$

o que é absurdo, porque $p > 1$ e o único divisor positivo de 1 é o próprio 1. Logo, qualquer que seja o *primo* p_n existe um *primo maior* que p_n, isto é, o conjunto

$$\{ 2,3,5,7,11,13,\ldots \}$$

dos *primos* é *infinito*.

<u>Teorema 7.4</u> Se um inteiro positivo $a > 1$ é *composto*, então <u>a</u> possui um *divisor primo* $p \leqslant \sqrt{a}$.

<u>Demonstração:</u>

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

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

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

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

Por ser $b > 1$, o *"Teorema fundamental da Aritmética"* assegura que <u>b</u> tem pelo menos um *divisor primo* <u>p</u>, de modo que $p \leqslant b \leqslant \sqrt{a}$. E como $p|b$ e $b|a$, segue-se que $p|a$, isto é, o inteiro *primo* $p \leqslant \sqrt{a}$ é um *divisor* de <u>a</u>.

NOTA. O teorema anterior fornece um *processo* que permite reconhecer se um dado inteiro $a > 1$ é *primo* ou é *composto*, para o que basta dividir <u>a</u> sucessivamente pelos *primos* que não excedem a $\sqrt{a}$.

Assim, p.ex., no caso do inteiro $a = 509$, temos:

$$22 < \sqrt{509} < 23$$

de modo que os *primos* que não excedem a $\sqrt{509}$ são 2,3,5,7, 11,13,17 e 19, e como 509 não é divisível por nenhum deles, segue-se que 509 é *primo*.

Este processo, como logo se vê, é muito trabalhoso e, portanto, pouco prático, sendo até de aplicação impossível para inteiros muito grandes.

7.3 FÓRMULAS QUE DÃO PRIMOS

Os *primos* aparecem com muita irregularidade na sequência dos inteiros positivos, e por isso muitas fórmulas que dão *primos* foram construidas. Assim, p.ex., a fórmula de EULER:

$$f_n = n^2 + n + 41$$

fornece *primos* para $n = 0,1,2,\ldots,39$. Entretanto, para $n = 40$ e $n = 41$ os inteiros que se obtêm são *compostos*, pois, temos:

$$f_{40} = 40^2 + 40 + 41 = 40(40 + 1) + 41 = 40.41 + 41 =$$
$$= 41(40 + 1) = 41.41 = 41^2$$

$$f_{41} = 41^2 + 41 + 41 = 41(41 + 1) + 41 = 41.42 + 41 =$$
$$= 41(42 + 1) = 41.43$$

Outras fórmulas que dão *primos* são:

$$f_n = 2n^2 + 29 \quad \text{para} \quad 0 \leqslant n \leqslant 28$$

$$f_n = n^2 + n + 17 \quad \text{para} \quad 0 \leqslant n \leqslant 16$$

$$f_n = 3n^2 + 3n + 23 \quad \text{para} \quad 0 \leqslant n \leqslant 21$$

7.4 CRIVO DE ERATÓSTENES

A construção de uma *tabela* de *primos* que não excedem um dado inteiro n faz-se usando o processo conhecido pelo nome de *crivo de ERATÓSTENES*, e que consiste no seguinte: escrevem-se na ordem natural todos os inteiros desde 2 até n e, em seguida, *eliminam-se* todos os inteiros *compostos* que são múltiplos dos *primos* p tais que $p \leqslant \sqrt{n}$, isto é, $2p$, $3p$, $4p$, ...

Exemplo 7.3 Construir a *tabela* de todos os *primos* menores que 100.

Os *primos* p tais que $p \leqslant \sqrt{100} = 10$ são 2,3,5 e 7. Logo, cumpre escrever na ordem natural todos os inteiros desde 2 até 100 e, em seguida, *eliminar* todos os inteiros *compostos* que são múltiplos de 2,3,5 e 7.

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Os inteiros positivos *não eliminados:*

2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,
59,61,67,71,73,79,83,89,97

são todos os primos menores que 100.

7.5 PRIMOS GÊMEOS

<u>Definição 7.2</u> Chamam-se *primos gêmeos* dois inteiros positivos ímpares e consecutivos que são ambos *primos*.

Assim, p.ex., são pares de *primos gêmeos:*

3 e 5, 5 e 7, 11 e 13, 17 e 19, 29 e 31

Não se sabe até hoje se há um número infinito de pares de

primos gêmeos, mas são conhecidos *primos gêmeos* muito grandes, tais como:

140.737.488.353.507 e 140.737.488.353.509
140.737.488.353.699 e 140.737.488.353.701

Um fato interessante é a existência de apenas um terno de inteiros positivos ímpares e consecutivos que são todos primos: 3, 5 e 7.

7.6 SEQUÊNCIAS DE INTEIROS CONSECUTIVOS COMPOSTOS

Teorema 7.5 Existem sequências de n inteiros positivos consecutivos e *compostos*, qualquer que seja o inteiro positivo n.

Demonstração:

Com efeito, é óbvio que na sequência:

$$(n+1)! + 2,\ (n+1)! + 3,\ (n+1)! + 4, \ldots, (n+1)! + (n+1)$$

os seus n termos são inteiros positivos consecutivos, e cada um deles é *composto*, porque $(n+1)! + j$ é divisível por j se $2 \leqslant j \leqslant n+1$.

Assim, p.ex., supondo $n = 4$, obtemos a sequência:

$$5! + 2,\quad 5! + 3,\quad 5! + 4,\quad 5! + 5$$

cujos termos são 4 inteiros positivos consecutivos, cada um dos quais é *composto*, pois, temos:

$$5! + 2 = 122 = 2.61, \quad 5! + 3 = 123 = 3.41$$

$$5! + 4 = 124 = 4.31, \quad 5! + 5 = 125 = 5.25$$

Outras sequências de 4 inteiros positivos consecutivos e *compostos* existem, tais como

24, 25, 26, 27 e 32, 33, 34, 35

54, 55, 56, 57 e 74, 75, 76, 77

7.7 CONJECTURA DE GOLDBACH

No século XVIII o matemático CHRISTIAN GOLDBACH, numa carta a EULER, *conjecturou* que *todo inteiro par maior que 4 pode ser expresso como soma de dois primos ímpares*. Assim, p.ex., temos:

$$6 = 3 + 3$$

$$8 = 3 + 5$$

$$10 = 3 + 7 = 5 + 5$$

$$12 = 5 + 7$$

$$14 = 3 + 11 = 7 + 7$$

$$16 = 3 + 13 = 5 + 11$$

$$18 = 5 + 13 = 7 + 11$$

.....

Muitos matemáticos têm procurado demonstrar ou refutar a *conjectura de GOLDBACH*, mas nada foi conseguido até hoje.

NOTA. Um grande número de problemas interessantes relacionados com os primos permanece sem solução, tais como, p. ex., os dois seguintes:

(1) Há um número infinito de *primos* da forma $n^2 + 1$, onde $\underline{n}$ é um inteiro?

(2) Existe sempre pelo menos um primo entre n^2 e n^2+n para todo inteiro $n > 1$?

Há também muitas proposições sobre os *primos* cuja demonstração exige recursos de índole muito elevada, isto é, para as quais não existe uma demonstração elementar, tais como, p.ex., as duas seguintes:

(i) Em toda progressão aritmética:

$$a,\ a+r,\ a+2r,\ a+3r,\ \ldots$$

onde $\underline{a}$ e $\underline{r}$ (razão) são inteiros positivos *primos entre si*, há um número infinito de *primos* (DIRICHLET).

(ii) Para todo inteiro $n > 3$, entre $\underline{n}$ e $2(n-1)$ existe, pelo menos, um *primo* (TSCHEBISCHEFF).

7.8 MÉTODO DE FATORAÇÃO DE FERMAT

Dado um inteiro positivo *ímpar* $\underline{n}$, a decomposição de $\underline{n}$ num produto de *dois* fatores distintos se pode obter pelo seguinte método devido a FERMAT:

Constroi-se uma *tabela* com $(n-1)/2$ *linhas*, obtidas pela adição sucessiva de inteiros ímpares consecutivos a $\underline{n}$. Se na r-ésima linha aparece o *quadrado perfeito* t^2, então $n = (t + r)(t - r)$.

Assim, p.ex., com $n = 21$, temos a seguinte tabela de $(21 - 1)/2 = 10$ linhas:

1	$21 + 1 = \cancel{32}\ 22$
2	$22 + 3 = 25 = 5^2$
3	$25 + 5 = 30$
4	$30 + 7 = 37$
5	$37 + 9 = 46$
6	$46 + 11 = 57$
7	$57 + 13 = 70$
8	$70 + 15 = 85$
9	$85 + 17 = 102$
10	$102 + 19 = 121 = 11^2$

Na *segunda linha* figura 5^2 e na *décima linha* figura 11^2, de modo que temos:

$$21 = (5 + 2)(5 - 2) = 7 \times 3$$

$$21 = (11 + 10)(11 - 10) = 21 \times 1$$

São estas as *duas únicas* maneiras de decompor o inteiro positivo ímpar 21 num produto de dois fatores distintos, pois, todas as outras são variações triviais destas, tais como $21 = 3 \times 7 = (-7)(-3)$.

EXERCÍCIOS

1. Achar os cinco menores *primos* da forma $n^2 - 2$.

2. Achar três *primos ímpares* cuja soma seja:
   (a) 81; (b) 125

3. Achar todos os pares de *primos* p e q tais que $p - q = 3$.

4. Achar todos os *primos* que são iguais a um *quadrado perfeito* menos 1.

5. Achar todos os *primos* que são iguais a um *cubo perfeito* menos 1.

6. Determinar todos os inteiros positivos n tais que n, n+2 e n+4 são todos *primos*.

7. Determinar todos os *primos* p tais que 3p+1 é um *quadrado perfeito*.

8. Determinar se são *primos* os seguintes inteiros:

(a) 169 (c) 239

(b) 197 (d) 473

9. Achar a *decomposição canônica* do inteiro 5040.

10. Achar o mdc(a,b) e o mmc(a,b) sabendo:

$a = 2^{30}.5^{21}.19.23^3$ e $b = 2^6.3.7^4.11^2.19^5.23^7$

11. Mostrar que são *primos gêmeos:*

(a) 1949 e 1951 (b) 1997 e 1999

12. Achar todos os pares de *primos gêmeos* entre 400 e 500.

13. Achar uma sequência de quatro inteiros positivos consecutivos e *compostos*.

14. Achar uma sequência de 100 inteiros positivos consecutivos e *compostos*.

15. Verificar a *conjectura de GOLDBACH* para os seguintes inteiros *pares:*

(a) 32; (b) 100; (c) 456; (d) 1024.

16. Verificar que todo inteiro *par* entre 4 e 100 é a soma de dois *primos*.

17. Achar o *menor* inteiro positivo n tal que $2n^2 + 29$ é um inteiro *composto*.

18. Mostrar que a soma de inteiros positivos ímpares e consecutivos é sempre um inteiro *composto*.

19. Usando a *decomposição canônica* dos inteiros 507 e 1287, achar o mdc(507, 1287) e o mmc(507, 1287).

20. Demonstrar que todo *primo*, exceto 2 e 3, é da forma 6k-1 ou 6k+1, onde k é um inteiro positivo.

21. Achar o menor inteiro positivo pelo qual se deve dividir 3720 para se obter um *quadrado perfeito*.

22. Achar todos os *primos* que são *divisores* de 50!

23. Mostrar que o único *primo* da forma $n^3 - 1$ é 7.

24. Mostrar que todo inteiro da forma $n^4 + 4$, com $n > 1$, é *composto*.

25. Mostrar que, se $n > 4$, é *composto*, então n divide $(n - 1)!$

26. Mostrar que todo inteiro da forma $8^n + 1$, com $n \geq 1$, é *composto*.

27. Mostrar que, se n^2+2 é *primo*, então $3|n$.

28. Mostrar, mediante um exemplo, que a seguinte *conjectura é falsa:*

Todo inteiro positivo pode escrever-se sob a forma a^2+p, onde o inteiro $a \geqslant 0$ e $\underline{p}$ é um *primo* ou 1.

29. Demonstrar as seguintes proposições:

(a) Todo *primo* da forma $3n+1$ também é da forma $6m+1$.

(b) Todo inteiro da forma $3n+2$ tem um *fator primo* desta forma.

(c) Se $p \geqslant 5$ é um *primo*, então p^2+2 é *composto*.

(d) Se $\underline{p}$ é um *primo* e se $p|a^n$, então $p^n|a^n$.

(e) Todo inteiro $n > 11$ pode ser expresso como a soma de dois inteiros *compostos*.

(f) Se $p \geqslant q \geqslant 5$ e se $\underline{p}$ e $\underline{q}$ são ambos *primos*, então $24|(p^2 - q^2)$.

(g) Se $p \neq 5$ é um *primo ímpar*, então p^2-1 ou p^2+1 é divisível por 10.

30. Verificar que todo inteiro pode escrever-se sob a forma $2^k m$, onde o inteiro $k \geqslant 0$ e $\underline{m}$ é um inteiro *ímpar*.

31. Demonstrar que um inteiro positivo $a > 1$ é um *quadrado perfeito* se e somente se todos os expoentes dos fatores primos da sua *decomposição canônica* são inteiros *pares*.

32. Demonstrar que, se o inteiro $\underline{n}$ é *composto*, então 2^{n-1} também é *composto*.

33. Demonstrar que, se o inteiro $n > 2$, então existe um *primo* $\underline{p}$ tal que $n < p < n!$.

34. Demonstrar que todo *primo ímpar* é da forma $4k+1$ ou $4k-1$, onde $\underline{k}$ é um inteiro positivo.

CAPÍTULO 8

EQUAÇÕES DIOFANTINAS LINEARES

8.1 GENERALIDADES

O tipo mais simples de *equação diofantina* é a equação *diofantina linear com duas incógnitas* x e y:

$$ax + by = c$$

onde a, b e c são inteiros dados, sendo $ab \neq 0$.

Todo par de *inteiros* x_o, y_o tais que $ax_o + by_o = c$ diz se uma *solução inteira* ou apenas uma *solução* da equação $ax + by = c$.

Consideremos, p.ex., a equação diofantina linear com duas incógnitas:

$$3x + 6y = 18$$

Temos:

$$3.4 + 6.1 = 18$$

$$3(-6) + 6.6 = 18$$

$$3.10 + 6(-2) = 18$$

Logo, os pares de inteiros:

$$4 \text{ e } 1, \quad -6 \text{ e } 6, \quad 10 \text{ e } -2$$

são *soluções* da equação $3x + 6y = 18$.

Existem equações diofantinas lineares com duas incógnitas que *não têm solução*. Assim, p.ex., a equação diofantina linear:

$$2x + 4y = 7$$

não tem solução, porque $2x + 4y$ é um inteiro par quaisquer que sejam os valores inteiros de $\underline{x}$ e $\underline{y}$, enquanto que 7 é um inteiro *ímpar* (observe-se que $2 = \text{mdc}(2,4)$ *não divide* 7).

De modo geral, a equação diofantina linear $ax + by = c$ *não tem solução* todas as vezes que $d = \text{mdc}(a,b)$ *não divide* $\underline{c}$, como é óbvio.

8.2 CONDIÇÃO DE EXISTÊNCIA DE SOLUÇÃO

<u>Teorema 8.1</u> A equação diofantina linear $ax + by = c$ tem *solução* se e somente se $\underline{d}$ *divide* $\underline{c}$, sendo $d = \text{mdc}(a,b)$.

Demonstração:

($\Longrightarrow$) Suponhamos que a equação $ax + by = c$ tem uma *solução*, isto é, que existe um par de inteiros x_o, y_o tais

que $ax_o + by_o = c$.

Por ser o $mdc(a,b) = d$, existem inteiros r e s tais que $a = dr$ e $b = ds$, e temos:

$$c = ax_o + by_o = drx_o + dsy_o = d(rx_o + sy_o)$$

E como $rx_o + sy_o$ é um inteiro, segue-se que d *divide* c $(d|c)$.

($\Longleftarrow$) Reciprocamente, suponhamos que d *divide* c $(d|c)$, isto é, que $c = dt$, onde t é um inteiro.

Por ser o $mdc(a,b) = d$, existem inteiros x_o e y_o tais que

$$d = ax_o + by_o$$

o que implica:

$$c = dt = (ax_o + by_o)\ t = a(tx_o) + b(ty_o)$$

isto é, o par de inteiros:

$$x = tx_o = (c/d)x_o, \quad y = ty_o = (c/d)y_o$$

é uma *solução* da equação $ax + by = c$.

8.3 SOLUÇÕES DA EQUAÇÃO $ax + by = c$.

Teorema 8.2 Se d *divide* c $|(d|c)$, sendo $d = mdc(a,b)$, e se o par de inteiros x_o, y_o é uma *solução particular* da

equação diofantina linear $ax + by = c$, então todas as outras *soluções* desta equação são dadas pelas fórmulas:

$$x = x_o + (b/d)t, \quad y = y_o - (a/d)t$$

onde t é um inteiro arbitrário.

Demonstração:

Suponhamos que o par de inteiros x_o, y_o é uma *solução particular* da equação $ax + by = c$, e seja x_1, y_1 uma outra *solução qualquer* desta equação. Então, temos:

$$ax_o + by_o = c = ax_1 + by_1$$

e, portanto:

$$a(x_1 - x_o) = b(y_o - y_1)$$

Por ser o $mdc(a,b) = d$, existem inteiros r e s tais que $a = dr$ e $b = ds$, com r e s *primos entre si*. Substituindo estes valores de a e b na igualdade anterior e *cancelando* o fator com d, obtemos:

$$r(x_1 - x_o) = s(y_o - y_1)$$

Assim sendo, $r|s(y_o - y_1)$, e como o $mdc(r,s) = 1$, segue-se que $r|(y_o - y_1)$, isto é:

$$y_o - y_1 = rt \quad e \quad x_1 - x_o = st$$

onde t é um inteiro. Portanto, temos as fórmulas:

$$x_1 = x_o + st = x_o + (b/d)t$$

$$y_1 = y_o - rt = y_o - (a/d)t$$

Estes valores de x_1 e y_1 satisfazem realmente a equação $ax + by = c$, qualquer que seja o inteiro $\underline{t}$, pois, temos:

$$ax_1 + by_1 = a\left[x_o + (b/d)t\right] + b\left[y_o - (a/d)t\right] =$$

$$= (ax_o + by_o) + (ab/d - ab/d)t =$$

$$= c + 0.t = c$$

Como se vê, se $d = mdc(a,b)$ *divide* $\underline{c}$ $(d|c)$, então a equação diofantina linear $ax + by = c$ admite um número infinito de soluções, uma para cada valor do inteiro arbitrário $\underline{t}$.

<u>Corolário 8.1</u> Se o $mdc(a,b) = 1$ e se x_o, y_o é uma *solução particular* da equação diofantina linear $ax + by = c$, então todas as outras soluções desta equação são dadas pelas fórmulas:

$$x = x_o + \underset{(a,b)}{\underline{b}}t, \quad y = y_o - at$$

onde $\underline{t}$ é um inteiro arbitrário.

NOTA. Uma *solução particular* da equação diofantina linear se obtém por *tentativas* ou pelo *algoritmo de EUCLIDES*. E em ambos os casos a *solução geral* se pode obter usando o teorema 8.2, conforme se vai ver nos exemplos a seguir.

Exemplo 8.1 Determinar todas as *soluções* da equação diofantina linear,

$$172x + 20y = 1000$$

Determinemos, inicialmente, o mdc(172,20) pelo *algoritmo de EUCLIDES:*

$$172 = 20.8 + 12$$

$$20 = 12.1 + 8$$

$$12 = 8.1 + 4$$

$$8 = 4.2$$

Portanto, o mdc(172,20) = 4 e como $4|1000$, segue-se que a equação dada tem solução.

Posto isto, cumpre obter a expressão do inteiro 4 como *combinação linear de* 172 e 20, para que o que basta eliminar sucessivamente os *restos* 8 e 12 entre as três primeiras igualdades anteriores do seguinte modo:

$$4 = 12 - 8 = 12 - (20 - 12) = 2.12 - 20 =$$

$$= 2(172 - 20.8) - 20 = 172.2 + 20(-17)$$

isto é:

$$4 = 172.2 + 20(-17)$$

Multiplicando ambos os membros desta igualdade por 1000/4 = 250, obtemos:

$$1000 = 172.500 + 20(-4250)$$

Portanto, o par de inteiros $x_o = 500$, $y_o = -4250$ é uma *solução particular* da equação proposta, e todas as outras soluções são dadas pelas fórmulas:

$$x = 500 + (20/4)t = 500 + 5t$$

$$y = -4250 - (172/4)t = -4250 - 43t$$

onde t é um inteiro arbitrário.

Exemplo 8.2 Determinar todas as soluções *inteiras e positivas* da equação diofantina linear

$$18x + 5y = 48$$

Determinemos o mdc(18,5) pelo *algoritmo de EUCLIDES:*

$$18 = 5.3 + 3$$
$$5 = 3.1 + 2$$
$$3 = 2.1 + 1$$
$$2 = 1.2$$

	3	1	1	2
18	5	3	2	1
3	2	1	0	

Portanto, o mdc(18,5) = 1 e a equação dada tem *solução*. E para exprimir 1 como *combinação linear de* 18 e 5 basta eliminar os *restos* 2 e 3 entre as três primeiras igualdades anteriores do seguinte modo:

$$1 = 3 - 2 = 3 - (5 - 3) = 2.3 - 5 =$$

$$= 2(18 - 5.3) - 5 = 18.2 + 5(-7)$$

isto é:

$$1 = 18.2 + 5(-7)$$

e

$$48 = 18.96 + 5(-336)$$

Logo, o par de inteiros $x_o = 96$, $y_o = -336$ é uma *solução particular* da equação proposta, e todas as demais soluções são dadas pelas fórmulas:

$$x = 96 + 5t, \quad y = -336 - 18t$$

onde $\underline{t}$ é um inteiro arbitrário.

As soluções *inteiras e positivas* se acham escolhendo $\underline{t}$ de modo que sejam satisfeitas as desigualdades:

$$96 + 5t > 0, \qquad -336 - 18t > 0$$

isto é:

$$t < -19\,\frac{1}{5} \quad \text{e} \quad t < -18\,\frac{2}{3}$$

o que implica $t = -19$ e, portanto:

$$x = 96 + 5(-19) = 1, \quad y = -336 - 18(-19) = 6$$

Assim, o par de inteiros $x = 1$, $y = 6$ é a *única* solução *inteira e positiva* da equação $18x + 5y = 48$.

<u>Exemplo 8.3</u> Resolver a equação diofantina linear

$$39x + 26y = 105.$$

O mdc(39, 26) = 13 e como 13 não divide 105, segue-se que a equação dada *não tem solução*.

Exemplo 8.4 Resolver a equação diofantina linear

$$14x + 22y = 50.$$

O mdc(14, 22) = 2 e como $2|50$, a equação dada tem solução, e por simples inspeção logo se vê que

$$14.2 + 22.1 = 50,$$

de modo que o par de inteiros $x_o=2$, $y_o=1$ é uma *solução particular*, e por conseguinte todas as demais soluções são dadas pelas fórmulas:

$$x = 2 + 11t, \quad y = 1 - 7t$$

onde t é um inteiro arbitrário.

EXERCÍCIOS

1. Determinar todas as *soluções inteiras* das seguintes equações diofantinas lineares:

(a) $56x + 72y = 40$ (b) $24x + 138y = 18$

(c) $221x + 91y = 117$ (d) $84x - 438y = 156$

(e) $48x + 7y = 5$ (f) $57x - 99y = 77$

(g) $11x + 30y = 31$ (h) $27x - 18y = 54$

(i) $13x - 7y = 21$ (j) $44x + 66y = 11$

(k) $21x - 12y = 72$ (l) $17x + 54y = 8$

2. Determinar todas as *soluções inteiras e positivas* das seguintes equações diofantinas lineares:

(a) $5x - 11y = 29$

(b) $32x + 55y = 771$

(c) $58x - 87y = 290$

(d) $62x + 11y = 788$

(e) $30x + 17y = 300$

(f) $54x + 21y = 906$

(g) $123x + 360y = 99$

(h) $158x - 57y = 7$

3. Determinar o *menor* inteiro positivo que dividido por 8 e por 15 deixa os *restos* 6 e 13, respectivamente.

4. Exprimir 100 como soma de dois inteiros positivos de modo que o primeiro seja divisível por 7 e o segundo seja divisível por 11.

5. Determinar as duas menores frações positivas que tenham 13 e 17 para denominadores e cuja soma seja igual a 305/221.

6. Demonstrar que, se a e b são inteiros positivos *primos entre si*, então a equação diofantina $ax - by = c$ tem um número infinito de *soluções inteiras e positivas*.

CAPÍTULO 9

CONGRUÊNCIAS

9.1 INTEIROS CONGRUENTES

Definição 9.1 Sejam a e b dois inteiros quaisquer e seja m um inteiro *positivo fixo*. Diz-se que a *é congruente a* b *módulo* m se e somente se m divide a diferença a-b.

Em outros termos, a *é congruente a* b *módulo* m se e somente se existe um inteiro k tal que $a - b = km$.

Com a notação

$$a \equiv b \pmod{m}$$

indica-se que a *é congruente a* b *módulo* m. Portanto, simbolicamente:

$$a \equiv b \pmod{m} \Longleftrightarrow m \mid (a - b)$$

ou seja:

$$a \equiv b \pmod{m} \Longleftrightarrow \exists\, k \in \mathbb{Z} \mid a - b = km$$

Assim, p.ex.:

$$3 \equiv 24 \pmod{7}, \text{ porque } 7 \mid (3 - 24)$$

$$-31 \equiv 11 \pmod{6}, \text{ porque } 6 \mid (-31 - 11)$$

$$-15 \equiv -63 \pmod{8} \text{ porque } 8 \mid (-15 - (-63))$$

Se m não divide a diferença a-b, então diz-se que a *é incongruente a* b *módulo m*, o que se indica pela notação:

$$a \not\equiv b \pmod{m}$$

Assim, p.ex.:

$$25 \not\equiv 12 \pmod{7}, \text{ porque } 7 \nmid (25 - 12)$$

$$-21 \not\equiv 10 \pmod{5}, \text{ porque } 5 \nmid (-21 - 10)$$

$$16 \not\equiv 9 \pmod{4}, \text{ porque } 4 \nmid (16 - 9)$$

Note-se que dois inteiros quaisquer são congruentes *módulo* 1, enquanto que dois inteiros são congruentes *módulo* 2 se ambos são *pares* ou se ambos são *ímpares*.

Em particular, $a \equiv 0 \pmod{m}$ se e somente se o *módulo m divide* a ($m \mid a$).

Exemplo 9.1 Mostrar:

$$n \equiv 7 \pmod{12} \Longrightarrow n \equiv 3 \pmod{4}, \quad \forall\, n \in Z$$

Com efeito:

$$n \equiv 7 \pmod{12} \Longrightarrow n - 7 = 12k \Longrightarrow n - 3 = 4(3k+1)$$

$$4 \mid (n - 3) \Longrightarrow n \equiv 3 \pmod{4}$$

Exemplo 9.2 Mostrar:

$$n^2 \equiv 0 \pmod{4} \quad \text{ou} \quad n^2 \equiv 1 \pmod{4}, \qquad \forall n \in Z$$

Com efeito:

(i) n par: $n = 2k \Longrightarrow n^2 - 4k^2 \Longrightarrow 4 \mid n^2$

$$\Longrightarrow n^2 \equiv 0 \pmod{4}$$

(ii) n impar: $n = 2k+1 \Longrightarrow n^2 = 4(k^2+k) + 1$

$$\Longrightarrow 4 \mid (n^2-1) \Longrightarrow n^2 \equiv 1 \pmod{4}$$

9.2 CARACTERIZAÇÃO DE INTEIROS CONGRUENTES

Teorema 9.1 Dois inteiros a e b são *congruentes módulo m* se e somente se a e b deixam o mesmo *resto* quando divididos por m.

Demonstração:

($\Longrightarrow$) Suponhamos que $a \equiv b \pmod{m}$. Então, por definição:

$$a - b = km, \quad \text{com} \quad k \in Z$$

Seja r o *resto* da divisão de b por m; então, pelo *algoritmo da divisão:*

$$b = mq + r, \quad \text{onde} \quad 0 \leqslant r < m$$

Portanto:

$$a = km + b = km + mq + r = (k + q)m + r$$

e isto significa que r é o *resto* da divisão de a por m, isto é, os inteiros a e b divididos por m deixam o mesmo *resto r*.

($\Longleftarrow$) Reciprocamente, suponhamos que a e b divididos por m deixam o mesmo *resto r*. Então, podemos escrever:

$$a = mq_1 + r \quad e \quad b = mq_2 + r, \quad \text{onde} \quad 0 \leqslant r < m$$

e, portanto:

$$a - b = (q_1 - q_2)m \Longrightarrow m|(a-b) \Longrightarrow a \equiv b \pmod{m}$$

Exemplo 9.3 Sejam os inteiros -56 e -11. Pelo algoritmo da divisão:

$$-56 = 9(-7) + 7 \quad e \quad -11 = 9(-2) + 7$$

isto é, -56 e -11 divididos por 9 deixam o mesmo *resto* 7. Logo, pelo teorema anterior: $-56 \equiv -11 \pmod{9}$.

Sejam, agora, os inteiros -31 e 11. Temos a congruência:

$$-31 \equiv 11 \pmod{7}$$

de modo que, pelo teorema anterior, -31 e 11 divididos por 7 deixam o mesmo *resto*. Realmente, é o que mostram as igualdades:

$$-31 = 7(-5) + 4 \quad e \quad 11 = 7.1 + 4$$

9.3 PROPRIEDADES DAS CONGRUÊNCIAS

Teorema 9.2 Seja m um inteiro *positivo fixo* ($m > 0$) e sejam a, b e c inteiros quaisquer. Subsistem as seguintes propriedades:

(1) $a \equiv a \pmod{m}$

(2) Se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$

(3) Se $a \equiv b \pmod{m}$ e se $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$.

Demonstração:

(1) Com efeito:

$$m|0 \text{ ou } m|(a - a) \Longrightarrow a \equiv a \pmod{m}$$

(2) Com efeito, se $a \equiv b \pmod{m}$, então $a - b = km$, com $k \in Z$.

Portanto:

$$b - a = -(km) = (-k)m \Longrightarrow b \equiv a \pmod{m}$$

(3) Com efeito, se $a \equiv b$ (mod. m) e se $b \equiv c$ (mod. m), então existem inteiros h e k tais que

$$a - b = hm \quad e \quad b - c = km$$

Portanto:

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

e isto significa que $a \equiv c$ (mod. m).

NOTA. Consoante este teorema, a relação R no conjunto Z dos inteiros definida por

$$aRb \Longleftrightarrow a \equiv b \text{ (mod. m)}$$

é *reflexiva, simétrica* e *transitiva,* ou seja, R é uma *relação de equivalência em* Z.

Esta relação de equivalência R em Z é denominada *"congruência módulo m"*.

Teorema 9.3 Seja m um inteiro *positivo fixo* ($m > 0$) e sejam a e b dois inteiros quaisquer. Subsistem as seguintes propriedades:

(1) Se $a \equiv b$ (mod. m) e se $n|m$, com $n > 0$, então $a \equiv b$ (mod. n)

(2) Se $a \equiv b$ (mod. m) e se $c > 0$, então $ac \equiv bc$ (mod. mc).

(3) Se $a \equiv b$ (mod. m) e se a, b, m são todos *divisíveis* pelo inteiro $d > 0$, então $a/d \equiv b/d$ (mod. m/d).

Demonstração:

(1) Com efeito:

$$a \equiv b \pmod{m} \Longrightarrow a - b = km \quad e \quad n|m \Longrightarrow m = nq$$

onde k e $q > 0$ são inteiros.

Portanto:

$$a - b = (kq)n \Longrightarrow a \equiv b \pmod{n}$$

(2) Com efeito:

$$a \equiv b \pmod{m} \Longrightarrow a - b = km \Longrightarrow ac - bc = k(mc)$$

$$\Longrightarrow ac \equiv bc \pmod{mc}$$

(3) Com efeito:

$$a \equiv b \pmod{m} \Longrightarrow a-b = km \Longrightarrow a/d - b/d = k(m/d)$$

$$\Longrightarrow a/d \equiv b/d \pmod{m/d}$$

Assim, p.ex.:

$$-15 \equiv 9 \pmod{8} \Longrightarrow -15 \equiv 9 \pmod{4}$$

$$7 \equiv -8 \pmod{3} \Longrightarrow 35 \equiv -40 \pmod{15}$$

$$36 \equiv -24 \pmod{12} \Longrightarrow 9 \equiv -6 \pmod{3}$$

Teorema 9.4 Seja m um inteiro *positivo fixo* ($m > 0$) e sejam a, b, c, d inteiros quaisquer. Subsistem as seguintes propriedades:

(1) Se $a \equiv b \pmod{m}$ e se $c \equiv d \pmod{m}$, então $a + c \equiv b + d \pmod{m}$ e $ac \equiv bd \pmod{m}$

(2) Se $a \equiv b \pmod{m}$, então $a + c \equiv b + c \pmod{m}$ e $ac \equiv bc \pmod{m}$

(3) Se $a \equiv b \pmod{m}$, então $a^n \equiv b^n \pmod{m}$ para todo inteiro positivo n.

Demonstração:

(1) Com efeito, se $a \equiv b \pmod{m}$ e se $c \equiv d \pmod{m}$, então existem inteiros h e k tais que $a - b = hm$ e $c - d = km$. Portanto:

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

e

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

o que implica:

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

(2) Com efeito, se $a \equiv b \pmod{m}$, como $c \equiv c \pmod{m}$, temos, pela propriedade anterior:

$$a + c \equiv b + c \pmod{m} \quad e \quad ac \equiv bc \pmod{m}$$

(3) Usando o *"Teorema da indução matemática"*, a proposição é verdadeira para $n = 1$, e suposta verdadeira para um inteiro positivo $\underline{k}$, temos:

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

Portanto, pela propriedade (1):

$$a^k.a \equiv b^k.b \pmod{m} \quad ou \quad a^{k+1} \equiv b^{k+1} \pmod{m}$$

isto é, a proposição é verdadeira para o inteiro positivo $k+1$. Logo, a proposição é verdadeira para todo inteiro positivo $\underline{n}$.

Assim, p.ex.:

(i) $12 \equiv 22 \pmod{5}$ e $8 \equiv 13 \pmod{5}$ implica:

$$12 + 8 \equiv 22 + 13 \pmod{5} \quad ou \quad 20 \equiv 35 \pmod{5}$$

e

$$12.8 \equiv 22.13 \pmod{5} \quad ou \quad 96 \equiv 286 \pmod{5}$$

(ii) $12 \equiv 5 \pmod{7}$ implica:

$$12 + 6 \equiv 5 + 6 \pmod{7} \quad ou \quad 18 \equiv 11 \pmod{7}$$

e

$$12(-9) \equiv 5(-9) \pmod{7} \quad ou \quad -108 \equiv -45 \pmod{7}$$

(iii) $-5 \equiv 2 \pmod{7}$ implica:

$$(-5)^3 \equiv 2^3 \pmod{7} \quad ou \quad -125 \equiv 8 \pmod{7}$$

Exemplo 9.4 Mostrar que $a \equiv b \pmod{m}$ implica

$$-a \equiv -b \pmod{m}.$$

Com efeito, multiplicando ordenadamente as congruências:

$$a \equiv b \pmod{m} \quad e \quad -1 \equiv -1 \pmod{m}$$

obtemos:

$$a(-1) \equiv b(-1) \pmod{m} \quad ou \quad -a \equiv -b \pmod{m}$$

Exemplo 9.5 Mostrar que $a + b \equiv c \pmod{m}$ implica

$$a \equiv c - b \pmod{m}.$$

Com efeito, somando ordenadamente as congruências:

$$a + b \equiv c \pmod{m} \quad e \quad -b \equiv -b \pmod{m}$$

obtemos:

$$a + b + (-b) \equiv c + (-b) \pmod{m} \quad ou \quad a \equiv c-b \pmod{m}$$

Portanto, numa congruência pode-se passar um termo de um membro para o outro trocando-lhe o sinal.

Teorema 9.5 Se $ac \equiv bc \pmod{m}$ e se o $mdc(c,m) = d$, então $a \equiv b \pmod{m/d}$.

Demonstração:

Com efeito, se $ac \equiv bc \pmod{m}$, então:

$$ac - bc = (a - b)c = km, \quad com \quad k \in Z$$

E se o mdc(c,m) = d, existem inteiros r e s tais que $c = dr$ e $m = ds$, onde r e s são *primos entre si*. Portanto:

$$(a - b)dr = kds \quad \text{ou} \quad (a - b)r = ks$$

o que implica que $s|(a - b)r$, com o $mdc(r,s) = 1$. Logo, pelo teorema 5.4 (DE EUCLIDES): $s|(a-b)$ e $a \equiv b \pmod{s}$ ou, por ser $s = m/d$, $a \equiv b \pmod{m/d}$.

Corolário 9.1 Se $ac \equiv bc \pmod{m}$ e se o $mdc(c,m) = 1$, então $a \equiv b \pmod{m}$.

Esta propriedade mostra que é permitido *cancelar* fatores de ambos os membros de uma congruência que são *primos* com o módulo.

Corolário 9.2 Se $ac \equiv bc \pmod{p}$, com p *primo*, e se p não divide c ($p \nmid c$), então $a \equiv b \pmod{p}$.

Demonstração:

Com efeito, as condições: p não divide c ($p \nmid c$) e p é *primo*, implicam que o $mdc(c,p) = 1$.

Exemplo 9.6 Consideremos a congruência:

$$33 \equiv 15 \pmod{9} \quad \text{ou} \quad 3.11 \equiv 3.5 \pmod{9}$$

Como o $mdc(3,9) = 3$, pelo teorema 9.5, temos:

$$11 \equiv 5 \pmod{3}.$$

Exemplo 9.7 Consideremos a congruência:

$$-35 \equiv 45 \pmod{8} \quad \text{ou} \quad 5(-7) \equiv 5.9 \pmod{8}$$

Como o mdc(5,8) = 1, podemos *cancelar* o fator 5 de ambos os membros da congruência, o que dá a nova congruência:

$$-7 \equiv 9 \pmod{8}.$$

Na congruência $4.11 \equiv 4.15 \pmod{8}$ não podemos *cancelar* o fator 4, porque o mdc(4,8) = 4 ≠ 1. Realmente, $11 \not\equiv 15 \pmod{8}$. Mas, temos $11 \equiv 15 \pmod{2}$

9.4 SISTEMAS COMPLETOS DE RESTOS

Definição 9.2 Chama-se *sistema completo de restos módulo m* todo conjunto $S = \{r_1, r_2, \ldots, r_m\}$ de m inteiros tal que um inteiro qualquer a é *congruente módulo m* a um *único* elemento de S.

Assim, p.ex., cada um dos conjuntos:

$$\{1,2,3\}, \quad \{0,1,2\}, \quad \{-1,0,1\}, \quad \{1,5,9\}$$

é um *sistema completo de restos módulo* 3.

Teorema 9.6 O conjunto $S = \{0,1,2,\ldots,m-1\}$ é um *sistema completo de restos módulo m.*

Demonstração:

Seja a um inteiro qualquer e sejam q e r o *quociente* e o *resto* na divisão de a pelo inteiro positivo m, isto é:

$$a = mq + r \ , \quad \text{onde} \quad 0 \leqslant r < m$$

Então, pela definição de inteiros congruentes módulo m, temos:

$$a \equiv r \ (\text{mod}.m)$$

e como r só pode assumir os valores $0,1,2,\ldots,m-1$, segue-se que o inteiro a é congruente módulo m a um *único* elemento do conjunto S, e por conseguinte este conjunto é um *sistema completo de restos módulo* m.

Assim, p.ex., o conjunto $S = \{0,1,2,3,4\}$ é um *sistema completo de restos módulo* 5.

Corolário 9.3 Se $S = \{r_1, r_2, \ldots, r_m\}$ é um *sistema completo de restos módulo* m, então os elementos de S são *congruentes módulo m aos inteiros* $0,1,2,\ldots,m-1$, tomados numa certa ordem.

Demonstração:

Com efeito, qualquer que seja o inteiro a, temos:

$$a \equiv r_i \ (\text{mod}.m), \quad \text{com} \quad r_i \in S$$

$$a \equiv k \ (\text{mod}.m), \quad \text{com} \quad 0 \leqslant k \leqslant m-1$$

Logo, pela propriedade transitiva da "congruência módulo m", temos:

$$r_i \equiv k \pmod{m}$$

Assim, p.ex., o conjunto:

$$S = \{-12, -4, 11, 13, 22, 82, 91\}$$

é um *sistema completo de restos módulo* 7, e temos:

$-12 \equiv 2 \pmod{7}$, $-4 \equiv 3 \pmod{7}$, $11 \equiv 4 \pmod{7}$

$13 \equiv 6 \pmod{7}$, $22 \equiv 1 \pmod{7}$, $82 \equiv 5 \pmod{7}$

$91 \equiv 0 \pmod{7}$.

isto é, os elementos de S são *congruentes módulo* 7 aos inteiros 2, 3, 4, 6, 1, 5, 0.

<u>Exemplo 9.8</u> Mostrar que o conjunto $S' = \{-2, -1, 0, 1, 2\}$ é um *sistema completo de restos módulo* 5.

Pelo teorema 9.6, um inteiro qualquer <u>a</u> é congruente módulo 5 a um *único* elemento do conjunto $\{0, 1, 2, 3, 4\}$, isto é:

$$a \equiv k \pmod{5}, \quad \text{com} \quad 0 \leqslant k \leqslant 4$$

Por outro lado, os elementos de S são congruentes módulo 5 aos inteiros 0,1,2,3,4, tomados numa certa ordem, pois, temos:

$$-2 \equiv 3 \pmod{5}, \quad -1 \equiv 4 \pmod{5}, \quad 0 \equiv 0 \pmod{5}$$

$$1 \equiv 1 \pmod{5}, \quad 2 \equiv 2 \pmod{5}$$

Logo, o inteiro a é congruente módulo 5 a um *único* elemento do conjunto S, e por conseguinte este conjunto é um *sistema completo de restos módulo* 5.

EXERCÍCIOS

1. Verdadeiro (V) ou falso (F):

   (a) $91 \equiv 0 \pmod{7}$ (b) $3 + 5 + 7 \equiv 5 \pmod{10}$

   (c) $-2 \equiv 2 \pmod{8}$ (d) $11^2 \equiv 1 \pmod{3}$

   (e) $17 \not\equiv 9 \pmod{2}$ (f) $42 \not\equiv -8 \pmod{10}$

2. Verdadeiro (V) ou falso (F):

   (a) $x \equiv 3 \pmod{5} \Longrightarrow x \in \{\ldots,-7,-2,3,8,13,\ldots\}$

   (b) $5 \equiv -1 \pmod{6}$ e $-1 \equiv -7 \pmod{6} \Longrightarrow 5 \equiv -7 \pmod{6}$

3. Achar o menor inteiro positivo que representa a soma:

   (a) $5 + 3 + 2 + 1 + 8 \pmod{7}$

   (b) $2 + 3 - 1 + 7 - 2 \pmod{4}$

4. Sabendo que $1066 \equiv 1776 \pmod{m}$, achar todos os possíveis valores do módulo $\underline{m}$.

5. Exprimir que "n é ímpar" de três outras maneiras.

6. Achar todos os inteiros $\underline{x}$ tais que $0 \leqslant x < 15$ e $3x \equiv 6 \pmod{15}$.

7. Achar todos os inteiros $\underline{x}$ tais que $1 \leqslant x \leqslant 100$ e $x \equiv 7 \pmod{17}$.

8. Sabendo que $k \equiv 1 \pmod{4}$, mostrar que $6k+5 \equiv 3 \pmod{4}$.

9. Mostrar, mediante um exemplo, que $a^2 \equiv b^2 \pmod{m}$ não implica $a \equiv b \pmod{m}$.

10. Mostrar que todo *primo* (exceto 2) é *congruente módulo* 4 a 1 ou 3.

11. Mostrar que todo *primo* (exceto 2 e 3) é *congruente módulo* 6 a 1 ou 5.

12. Mostrar que $11^{10} \equiv 1 \pmod{100}$.

13. Mostrar que 41 divide $2^{20} - 1$.

14. Achar os *restos* das divisões de 2^{50} e 41^{65} por 7.

15. Mostrar:

(a) $89 \mid (2^{44} - 1)$; (b) $97 \mid (2^{48} - 1)$.

16. Demonstrar que, se $a \equiv b \pmod{m}$, então o

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

17. Mostrar, mediante um exemplo, que $a^k \equiv b^k \pmod{m}$ e $k \equiv j \pmod{m}$ não implica $a^j \equiv b^j \pmod{m}$.

18. Demonstrar as seguintes proposições:

(a) Se $\underline{a}$ é um inteiro *ímpar*, então $a^2 \equiv 1 \pmod{8}$.

(b) Se $\underline{a}$ é um inteiro qualquer, então $a^3 \equiv 0,1$ ou $8 \pmod{9}$.

(c) Se $\underline{a}$ é um inteiro qualquer, então $a^3 \equiv a \pmod{6}$.

19. Determinar quais dos seguintes conjuntos são *sistemas completos de restos módulo* 4:

(a) $\{-2,-1,0,1\}$ (b) $\{0,4,8,12\}$

(c) $\{-13,4,17,18\}$ (d) $\{-5,0,6,22\}$

20. Determinar quais dos seguintes conjuntos são *sistemas completos de restos módulo* 6:

(a) $\{1,2,3,4,5\}$ (b) $\{0,5,10,15,20,25\}$

(c) $\{-4,-3,-2,-1,0,1\}$ (d) $\{17,-4,6,7,10,3\}$

21. Achar um *sistema completo de restos* $\{p_1,p_2,\ldots,p_7\}$ *módulo* 7 tal que todo p_i é *primo*.

22. Achar um *sistema completo de restos módulo* 7 formado só de múltiplos não negativos de 4.

CAPÍTULO 10

CONGRUÊNCIAS LINEARES

10.1 GENERALIDADES

Definição 10.1 Chama-se *congruência linear* toda equação da forma

$$ax \equiv b \pmod{m} \qquad (1)$$

onde a e b são dois inteiros quaisquer e m um inteiro *positivo*.

Todo inteiro x_o tal que

$$ax_o \equiv b \pmod{m}$$

diz-se uma *solução* da congruência linear (1).

Temos $ax_o \equiv b \pmod{m}$ se e somente se $m|(ax_o - b)$, isto é, se existe um inteiro y_o tal que $ax_o - b = my_o$, de modo que o problema de achar todos os inteiros que satisfazem a congruência linear (1) reduz-se ao de obter todas as *soluções* da equação diofantina linear $ax - my = b$.

É importante notar que, se x_o é uma *solução* da congruência linear (1), então todos os inteiros $x_o + km$, onde $\underline{k}$ é um inteiro arbitrário, isto é, os inteiros:

$$\ldots, x_o - 2m, x_o - m, x_o + m, x_o + 2m, \ldots$$

também são *soluções* da congruência linear (1), pois, temos:

$$a(x_o + km) \equiv ax_o \equiv b \pmod{m}$$

Consideremos, p.ex., a congruência linear:

$$3x \equiv 9 \pmod{12} \qquad (2)$$

Como $3.3 \equiv 9 \pmod{12}$, segue-se que $x_o = 3$ é uma *solução* desta congruência linear, e por conseguinte todos os inteiros $3 + 12k$, isto é, os inteiros:

$$\ldots, -33, -21, -9, 15, 27, 39, \ldots$$

também são *soluções* da congruência linear (2).

Como se vê, obtida uma *solução particular* x_o de uma congruência linear $ax \equiv b \pmod{m}$ podemos imediatamente construir uma indinidade de outras soluções, todas mutuamente congruentes módulo $\underline{m}$.

Duas soluções quaisquer da congruência linear (1), x_o e x_1, que são congruentes módulo $\underline{m}$, isto é, tais que $x_o \equiv x_1 \pmod{m}$, não são consideradas *soluções distintas*, isto é, o *número de soluções* da congruência linear (1) é dado pelo

número de soluções mutuamente incongruentes módulo m que a satisfazem.

Assim, p.ex., as *soluções* $x_o = 3$ e $x_1 = -9$ da congruência linear (2) são *congruentes módulo* 12 e, portanto, não são contadas como *soluções diferentes* desta congruência.

Finalmente, observaremos que uma congruência linear pode ter apenas *uma solução*, ou ter *várias soluções* ou *não ter soluções*, conforme se verá mais adiante.

10.2 CONDIÇÃO DE EXISTÊNCIA DE SOLUÇÃO

<u>Teorema 10.1</u> A congruência linear $ax \equiv b \pmod{m}$ tem *solução* se e somente se <u>d</u> *divide* <u>b</u> $(d|b)$, sendo $d = mdc(a,m)$.

<u>Demonstração:</u>

($\Longrightarrow$) Suponhamos que a congruência linear $ax \equiv b \pmod{m}$ tem como *solução* o inteiro x_o, isto é, que $ax_o \equiv b \pmod{m}$. Então, existe um inteiro y_o tal que

$$ax_o - b = my_o \quad \text{ou} \quad ax_o - my_o = b$$

e como $d|a$ e $d|m$, porque $d = mdc(a,m)$, segue-se que $d|(ax_o - my_o)$ e, portanto, $d|b$.

($\Longleftarrow$) Reciprocamente, suponhamos que $d|b$, isto é, que $b = dk$, onde $\underline{k}$ é um inteiro.

Como o $mdc(a,m) = d$, existem inteiros x_o e y_o tais que

$$ax_o + my_o = d$$

ou, multiplicando ambos os membros desta igualdade por $\underline{k}$:

$$a(kx_o) + m(ky_o) = dk = b$$

ou

$$a(kx_o) - b = m(-ky_o)$$

o que implica:

$$a(kx_o) \equiv b \pmod{m}$$

Portanto, o inteiro kx_o é uma *solução* da congruência linear

$$ax \equiv b \pmod{m}$$

10.3 SOLUÇÕES DA CONGRUÊNCIA $ax \equiv b \pmod{m}$

<u>Teorema 10.2</u> Se $\underline{d}$ *divide* $\underline{b}$ $(d|b)$, sendo $d = mdc(a,m)$, então a congruência linear

$$ax \equiv b \pmod{m}$$

tem precisamente $\underline{d}$ *soluções mutuamente incongruentes módulo* $\underline{m}$.

Demonstração:

Foi mostrado anteriormente que a congruência $ax \equiv b \pmod{m}$ é *equivalente* à equação diofantina linear $ax - my = b$, equação esta que tem *solução* se e somente se $d = mdc(a,m)$ *divide* b $(d|b)$. Além disso, como é sabido, se $d|b$ e se o par de inteiros x_o, y_o é uma *solução particular* da equação $ax - my = b$, então todas as outras *soluções* desta equação são dadas pelas fórmulas:

$$x = x_o + (m/d)t, \quad y = y_o + (a/d)t$$

onde t é um inteiro arbitrário.

Entre o número infinito de inteiros dados pela primeira dessas fórmulas consideremos somente aqueles que resultam de atribuir a t os valores: $0,1,2,\ldots,d-1$, isto é, os d inteiros:

$$x_o,\ x_o + m/d,\ x_o + 2(m/d),\ldots,\ x_o + (d-1)(m/d)$$

Posto isto, vamos mostrar que estes d inteiros são *mutuamente incongruentes módulo* m e que todos os outros inteiros dados pela fórmula $x = x_o + (m/d)t$ são *congruentes módulo* m a algum desses d inteiros. Com efeito, se fosse

$$x_o + (m/d)t_1 \equiv x_o + (m/d)t_2 \pmod{m}$$

onde $0 \leqslant t_1 < t_2 \leqslant d-1$, então, teríamos:

$$(m/d)t_1 \equiv (m/d)t_2 \pmod{m}$$

E como o $mdc(m/d,m) = m/d$, podemos *cancelar* o fator comum m/d, o que dá a congruência:

$$t_1 \equiv t_2 \pmod{d}$$

e isto significa que $d|(t_2 - t_1)$, o que é *impossível*, visto que $0 < t_2 - t_1 < d$.

Além disso, qualquer outro inteiro $x_o + (m/d)t$ é *congruente módulo* $\underline{m}$ a algum dos $\underline{d}$ inteiros acima enumerados. Com efeito, pelo algoritmo da divisão, temos:

$$t = dq + r, \quad \text{onde} \quad 0 \leqslant r \leqslant d-1$$

e, portanto:

$$x_o + (m/d)t = x_o + (m/d)(dq + r) = x_o + mq + (m/d)r$$

isto é:

$$x_o + (m/d)t \equiv x_o + (m/d)r \pmod{m}$$

onde $x_o + (m/d)r$ é um dos $\underline{d}$ inteiros que foram *selecionados*.

NOTA. Consoante a demonstração do teorema 10.2: se x_o é uma *solução* qualquer da congruência linear $ax \equiv b \pmod{m}$, então as suas $d = mdc(a,m)$ *soluções mutuamente incongruentes módulo* $\underline{m}$ são os inteiros:

$$x_o,\ x_o + m/d,\ x_o + 2(m/d), \ldots,\ x_o + (d-1)(m/d)$$

Corolário 10.1 Se o mdc(a,m) = 1, então a congruência linear $ax \equiv b \pmod{m}$ tem uma *única* solução módulo m.

Exemplo 10.1 Resolver a congruência linear

$$18x \equiv 30 \pmod{42}.$$

O mdc(18,42) = 6 e como $6|30$, a congruência dada tem exatamente 6 *soluções mutuamente incongruentes módulo* 42.

Como $18.4 \equiv 30 \pmod{42}$, uma *solução* da congruência dada é $x_o = 4$, e por conseguinte as suas 6 soluções mutuamente incongruentes módulo 42 são dadas pela fórmula:

$$x=4 + (42/6)t = 4 + 7t, \quad \text{onde} \quad t = 0,1,\ldots,5$$

isto é, são os inteiros:

$$x = 4, 11, 18, 25, 32, 39$$

Exemplo 10.2 Resolver a congruência linear $21x \equiv 15 \pmod{39}$.

O mdc(21,39) = 3 e como $3|15$, a congruência dada tem exatamente 3 *soluções mutuamente incongruentes módulo* 39.

Uma *solução* da congruência dada se pode obter resolvendo a equação diofantina linear $21x - 39y = 15$.

Pelo algoritmo de EUCLIDES, temos:

$$39 = 21.1 + 18$$
$$21 = 18.1 + 3$$
$$18 = 3.6$$

donde se deduz:

$$3 = 21 - 18 = 21 - (39 - 21) = 21.2 - 39$$

e

$$15 = 21.10 - 39.5$$

isto é, o par de inteiros $x_o = 10$, $y_o = 5$ é uma *solução particular* da equação diofantina linear $21x - 39y=15$ e, portanto, $x_o = 10$ é uma *solução* da congruência dada $21x \equiv 15 \pmod{39}$. Logo, as 3 *soluções mutuamente incongruentes módulo* 39 desta congruência são dadas pela fórmula:

$$x = 10 + (39/3)t = 10 + 13t, \text{ onde } t = 0,1,2$$

isto é, são os inteiros: $x = 10, 23, 36$.

<u>Exemplo 10.3</u> Resolver a congruência

$$11x \equiv 2 \pmod{317}.$$

O mdc(11,317) = 1 e, portanto, a congruência dada tem uma *única* solução módulo 317, que se pode obter resolvendo a equação diofantina linear $11x - 317y = 2$.

Pelo algoritmo de EUCLIDES, temos:

$$317 = 11.28 + 9$$

$$11 = 9.1 + 2$$

$$9 = 2.4 + 1$$

$$2 = 1.2$$

donde se deduz:

$$1 = 9 - 2.4 = 9 - (11 - 9)4 = 9.5 - 11.4 =$$

$$= (317 - 11.28)5 - 11.4 = 317.5 - 11.144$$

e

$$2 = 11(-288) - 317(-10)$$

Portanto, $x = -288$ ou $x = 29$ é a *única* solução módulo 317 da congruência $11x \equiv 2 \pmod{317}$.

<u>Exemplo 10.4</u> Resolver a congruência linear

$$36x \equiv 53 \pmod{131}.$$

O mdc(36,131) = 1 e, portanto, a congruência dada tem uma *única* solução módulo 131.

Como $53 \equiv -78 \pmod{131}$, temos:

$$36x \equiv -78 \pmod{131}$$

$$6.6x \equiv 6(-13) \pmod{131}$$

ou seja, por ser o mdc(6,131) = 1:

$$6x \equiv -13 \pmod{131}$$

Como $-13 \equiv -144 \pmod{131}$, temos:

$$6x \equiv -144 \pmod{131}$$

$$6x \equiv 6(-24) \pmod{131}$$

ou seja, por ser o mdc(6,131) = 1:

$$x \equiv -24 \equiv 107 \pmod{131}$$

<u>Exemplo 10.5</u> Resolver a congruência linear

$$35x \equiv 5 \pmod{14}.$$

O mdc(35,14) = 7 e como 7 *não divide* 5 ($7 \nmid 5$), a congruência dada *não tem solução*.

<u>Exemplo 10.6</u> Resolver a congruência linear

$$64x \equiv 16 \pmod{84}.$$

O mdc(64,84) = 4 e como $4 \mid 16$, a congruência dada tem precisamente 4 *soluções mutuamente incongruentes módulo* 84.

Temos:

$$16.4x \equiv 16.1 \pmod{84} \quad \text{e} \quad \text{mdc}(16,84) = 4$$

o que implica:

$$4x \equiv 1 \equiv -20 \pmod{21}$$

$$4x \equiv 4(-5) \pmod{21}$$

ou seja, por ser o $mdc(4,21) = 1$:

$$x \equiv -5 \equiv 16 \pmod{21}$$

Logo, as 4 soluções mutuamente incongruentes módulo 84 da congruência $64x \equiv 16 \pmod{34}$ são dadas pela fórmula:

$$x = 16 + (84/4)t = 16 + 21t, \quad \text{onde} \quad t = 0,1,2,3$$

isto é, são os inteiros: $x = 16, 37, 58, 79$.

10.4 RESOLUÇÃO DE EQUAÇÕES DIOFANTINAS LINEARES POR CONGRUÊNCIAS

Conforme foi demonstrado anteriormente (Teorema 8.1), a equação diofantina linear

$$ax + by = c \qquad (1)$$

tem *solução* se e somente se $d|c$, sendo $d = mdc(a,b)$. Neste caso, se o par de inteiros x_o, y_o é uma *solução particular* qualquer desta equação, então:

$$ax_o + by_o = c \quad e \quad ax_o - c = -by_o$$

o que implica:

$$ax_o \equiv c \pmod{b} \qquad (2)$$

Assim sendo, para obter uma *solução particular* da equação diofantina linear (1) basta determinar uma *solução* qualquer $x = x_o$ da congruência linear

$$ax \equiv c \pmod{b} \qquad (3)$$

e substituir este valor x_o de $\underline{x}$ na equação (1) afim de encontrar o valor correspondente y_o de $\underline{y}$, isto é, tal que $ax_o + by_o = c$.

Obviamente, também se pode obter uma *solução particular* da equação diofantina linear (1) determinando uma *solução* qualquer $y = y_o$ da congruência linear:

$$by \equiv c \pmod{a}$$

<u>Exemplo 10.7</u> Resolver por *congruências* a equação diofantina linear

$$48x + 7y = 17$$

Como o $mdc(48,7) = 1$, a equação dada tem *solução* e, portanto, para obter uma *solução particular* desta equação cumpre determinar uma *solução* qualquer da congruência linear:

$$48x \equiv 17 \pmod{7}$$

Por ser $48x \equiv -x \pmod{7}$, temos:

$$-x \equiv 17 \equiv 3 \pmod{7}$$
$$x \equiv -3 \equiv 4 \pmod{7}$$

Substituindo este valor $x = 4$ na equação diofantina linear dada, obtemos:

$$48.4 + 7y = 17 \Longrightarrow y = -25$$

Logo, o par de inteiros 4, -25 é uma *solução particular* da equação diofantina linear $48x + 7y = 17$, e todas as outras soluções são dadas pelas fórmulas:

$$x = 4 + 7t, \quad y = -25 - 48t$$

onde t é um inteiro arbitrário.

Exemplo 10.8 Resolver por *congruências* a equação diofantina linear:

$$9x + 16y = 35$$

A equação dada tem *solução* porque o $mdc(9,16) = 1$, e a congruência linear:

$$16y \equiv 35 \pmod{9} \quad \text{ou} \quad 7y \equiv 35 \pmod{9}$$

dá-nos:

$$y \equiv 5 \pmod{9} \Longrightarrow y = 5 + 9t$$

onde t é um inteiro arbitrário. Substituindo este valor de y na equação diofantina linear dada, obtemos:

$$9x + 16(5 + 9t) = 35 \Longrightarrow x = -5 - 16t$$

10.5 INVERSO DE UM INTEIRO

Definição 10.2 Seja $\underline{a}$ um inteiro. Chama-se *inverso de* $\underline{a}$ *módulo* $\underline{m}$ um inteiro a^* tal que $aa^* \equiv 1 \pmod{m}$.

Nem todo inteiro tem um *inverso módulo* $\underline{m}$. Assim, p.ex., 2 não tem um *inverso módulo* 4, porque a congruência linear $2x \equiv 1 \pmod{4}$ não tem solução.

Teorema 10.3 Se o $mdc(a,m) = 1$, então $\underline{a}$ tem um *único* inverso módulo m.

Demonstração:

Com efeito, se o $mdc(a,m) = 1$, então a congruência linear

$$ax \equiv 1 \pmod{m}$$

tem uma *única* solução $x_o \pmod{m}$, isto é:

$$ax_o \equiv 1 \pmod{m}$$

de modo que o inteiro $\underline{a}$ tem um *único inverso módulo* $\underline{m}$:

$$a^* = x_o.$$

Exemplo 10.9 Por ser $5.5 = 25 \equiv 1 \pmod{8}$, segue-se que o *inverso de* 5 *módulo* 8 é o próprio 5.

Note-se que

$$5(-3) \equiv 1 \pmod{8} \quad e \quad 5.13 \equiv 1 \pmod{8}$$

de modo que -3 e 13 também são *inversos* de 5 *módulo* 8, mas isto não é inconsistente com a *unicidade* do inverso de 5 módulo 8, porque

$$-3 \equiv 5 \equiv 13 \pmod{8}$$

Exemplo 10.10 Achar: (a) o inverso de 2 módulo 5: (b) o inverso de 7 módulo 9: (c) o inverso de 12 módulo 17.

Temos as congruências lineares:

$$2a^* \equiv 1 \pmod{5} \Longrightarrow a^* = 3$$

$$7a^* \equiv 1 \pmod{9} \Longrightarrow a^* = 4$$

$$12a^* \equiv 1 \pmod{17} \Longrightarrow a^* = 10$$

EXERCÍCIOS

1. Resolver as seguintes congruências lineares:

(a) $2x \equiv 1 \pmod{17}$	(b) $3x \equiv 1 \pmod{17}$
(c) $3x \equiv 6 \pmod{18}$	(d) $25x \equiv 15 \pmod{29}$
(e) $5x \equiv 2 \pmod{26}$	(f) $6x \equiv 15 \pmod{21}$
(g) $36x \equiv 8 \pmod{102}$	(h) $34x \equiv 60 \pmod{98}$
(i) $8x \equiv 16 \pmod{12}$	(j) $14x \equiv 36 \pmod{43}$

2. Resolver por *congruências* as seguintes equações diofantinas lineares:

(a) $4x + 51y = 9$ (b) $12x + 25y = 331$

(c) $5x - 53y = 17$ (d) $7x + 6y = 9$

(e) $11x + 27y = 4$ (f) $75x - 131y = 6$

(g) $39x + 26y = 104$ (h) $61x - 11y = 81$

(i) $65x + 77y = 200$ (j) $51x + 85y = 1037$

3. Determinar o *número de soluções* de cada uma das seguintes congruências lineares:

(a) $3x \equiv 6 \pmod{15}$ (b) $4x \equiv 8 \pmod{15}$

(c) $5x \equiv 10 \pmod{15}$ (d) $6x \equiv 11 \pmod{15}$

4. Determinar o *número de soluções* que pode ter uma congruência linear cujo módulo é 20.

5. Demonstrar que, se $d = mdc(a,m)$ e se $d|b$, então as congruências lineares:

$$ax \equiv b \pmod{m} \quad e \quad (a/d)x \equiv (b/d) \pmod{m/d}$$

têm precisamente as mesmas soluções.

CAPÍTULO 11

SISTEMAS DE CONGRUÊNCIAS LINEARES

11.1 GENERALIDADES

Um *sistema* de duas ou mais congruências lineares não tem necessariamente *solução*, mesmo que cada uma das congruências do sistema, isoladamente, tenha solução. Assim, p.ex., não existe inteiro algum $\underline{x}$ que verifique simultaneamente as congruências lineares:

$$x \equiv 1 \pmod{2} \quad \text{e} \quad x \equiv 0 \pmod{4}$$

embora cada uma delas, isoladamente, tenha solução.

Obviamente, um sistema de congruências lineares não tem solução se alguma das congruências do sistema não tem solução.

<u>Exemplo 11.1</u> Mostrar que todo inteiro $x \equiv 52 \pmod{105}$ *satisfaz* cada uma das três seguintes congruências lineares:

$$x \equiv 1 \pmod{3}$$
$$x \equiv 2 \pmod{5}$$
$$x \equiv 3 \pmod{7}$$

A primeira congruência dá-nos $x = 1 + 3a$, onde $\underline{a}$ é um inteiro. Substituindo este valor de $\underline{x}$ na segunda congruência, obtemos:

$$1 + 3a \equiv 2 \pmod{5}$$
$$3a \equiv 1 \pmod{5}$$
$$a \equiv 2 \pmod{5}$$

Portanto:

$$a = 2 + 5b \quad e \quad x = 1 + 3(2 + 5b) = 7 + 15b$$

onde $\underline{b}$ é um inteiro. Substituindo este valor de $\underline{x}$ na terceira congruência, obtemos:

$$7 + 15b \equiv 3 \pmod{7}$$
$$15b \equiv -4 \pmod{7}$$
$$b \equiv 3 \pmod{7}$$

Portanto:

$$b = 3 + 7c \quad e \quad x = 7 + 15(3 + 7c) = 52 + 105c$$

onde $\underline{c}$ é um inteiro, e isto significa que todo inteiro

$$x \equiv 52 \pmod{105}$$

satisfaz as três congruências lineares dadas.

Note-se que os módulos 3, 5 e 7 são *primos entre si dois a dois* e que o mmc(3,5,7) = 105.

11.2 TEOREMA DO RESTO CHINEZ

Sejam $m_1, m_2, \ldots, m_r$ inteiros positivos *primos entre si dois a dois*, isto é, tais que o $\text{mdc}(m_i, m_j) = 1$ se $i \neq j$. Nestas condições, o *sistema de congruências lineares:*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \ldots\ldots\ldots\ldots\ldots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

tem uma *única solução módulo* $m = m_1 m_2 \ldots m_r$.

<u>Demonstração:</u>

Para cada $k = 1, 2, \ldots, r$, seja:

$$M_k = m/m_k = m_1 m_2 \ldots m_{k-1} m_{k+1} \ldots m_r$$

isto é, M_k é o produto de todos os inteiros m_i com o fator m_k *omitido*. Por hipótese, os m_i são *primos entre si dois a dois*, de modo que o $\text{mdc}(M_k, m_k) = 1$ e, portanto, a congruência linear:

$$M_k x \equiv 1 \pmod{m_k} \qquad (1)$$

tem uma *única* solução x_k.

Posto isto, vamos demonstrar que o inteiro:

$$X = a_1M_1x_1 + a_2M_2x_2 + \ldots + a_rM_rx_r$$

satisfaz cada uma das congruências do sistema considerado, ou seja, que X é uma solução deste sistema.

Com efeito, se $i \neq k$, então $m_k | M_i$ e $M_i \equiv 0 \pmod{m_k}$, o que implica:

$$X = a_1M_1x_1 + a_2M_2x_2 + \ldots + a_rM_rx_r \equiv a_kM_kx_k \pmod{m_k}$$

E como x_k é a *solução* da congruência (1), temos

$$M_kx_k \equiv 1 \pmod{m_k}$$

o que implica:

$$X \equiv a_k.1 \equiv a_k \pmod{m_k}$$

e isto prova que X é uma *solução* do sistema de congruências lineares considerado.

Para demonstrar a *unicidade* desta *solução*, suponhamos que X_1 é uma outra *solução* qualquer do sistema de congruências considerado. Então:

$$X \equiv a_k \equiv X_1 \pmod{m_k}, \quad k = 1,2,\ldots,r$$

de modo que $m_k | (X - X_1)$ para cada valor de k. E como o $mdc(m_i,m_j) = 1$, segue-se que $m_1m_2\ldots m_r | (X - X_1)$, isto é:

$$m | (X - X_1) \quad e \quad X \equiv X_1 \pmod{m}$$

com o que termina a demonstração do *"Teorema do resto chinez"*.

<u>Exemplo 11.2</u> Resolver o sistema de congruências lineares:

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

Os *módulos* 3, 5 e 7 das congruências do sistema dado são *primos entre si dois a dois:*

$$\text{mdc}(3,5) = \text{mdc}(3,7) = \text{mdc}(5,7) = 1$$

de modo que, pelo teorema anterior, o sistema tem uma *única solução módulo* $m = 3.5.7 = 105$. Temos aqui:

$$M_1 = m/3 = 35, \quad M_2 = m/5 = 21, \quad M_3 = m/7 = 15$$

As congruências lineares:

$$35x \equiv 1 \pmod{3}, \quad 21x \equiv 1 \pmod{5}, \quad 15x \equiv 1 \pmod{7}$$

têm como *soluções* respectivas: $x_1 = 2$, $x_2 = 1$, $x_3 = 1$.

Portanto, o inteiro:

$$X = 2.35.2 + 3.21.1 + 2.15.1 = 233$$

Como $233 \equiv 23 \pmod{105}$, segue-se que $X \equiv 23 \pmod{105}$ é a *única solução* do sistema de congruências lineares dado.

Note-se que este sistema corresponde ao seguinte problema: achar um inteiro que deixa os restos 2, 3 e 2 quando dividido por 3, 5 e 7, respectivamente.

Exemplo 11.3 Resolver o sistema de congruências lineares:

$$\begin{cases} x \equiv 8 \pmod{5} \\ x \equiv 5 \pmod{3} \\ x \equiv 11 \pmod{7} \\ x \equiv 2 \pmod{4} \end{cases}$$

Os módulos 5,3,7 e 4 das congruências do sistema dado são *primos entre si dois a dois*, de modo que o sistema tem uma *única solução módulo* $m = 5.3.7.4 = 420$. Temos:

$$M_1 = m/5 = 84, \quad M_2 = m/3 = 140, \quad M_3 = m/7 = 60$$

$$M_4 = m/4 = 105$$

As congruências lineares:

$$84x \equiv 1 \pmod{5}, \quad 140x \equiv 1 \pmod{3}, \quad 60x \equiv 1 \pmod{7}$$

$$105x \equiv 1 \pmod{4}$$

tem como *soluções* respectivas: $x_1 = 4$, $x_2 = 2$, $x_3 = 2$, $x_4 = 1$.

Portanto, o inteiro:

$$X = 8.84.4 + 5.140.2 + 11.60.2 + 2.105.1 = 5618$$

Como $5618 \equiv 158 \pmod{420}$, segue-se que

$$X \equiv 158 \pmod{420}$$

é a *única solução* do sistema de congruências lineares dado.

<u>Teorema 11.1</u> Sejam $m_1, m_2, \ldots, m_r$ inteiros positivos *primos entre si dois a dois*, isto é, o $mdc(m_i, m_j) = 1$ se $i \neq j$, e sejam $a_1, a_2, \ldots, a_r$ inteiros tais que o

$$mdc(a_k, m_k) = 1 \quad \text{para} \quad k = 1, 2, \ldots, r$$

Nestas condições, o sistema de congruências lineares:

$$\begin{cases} a_1 x \equiv b_1 \pmod{m_1} \\ a_2 x \equiv b_2 \pmod{m_2} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_r x \equiv b_r \pmod{m_r} \end{cases}$$

tem uma *única solução módulo* $m = m_1 m_2 \ldots m_r$.

<u>Demonstração:</u>

Com o $mdc(a_k, m_k) = 1$, a congruência linear

$$a_k x \equiv 1 \pmod{m_k}$$

tem uma *única solução* módulo m_k: a_k^*, de modo que

$$a_k a_k^* \equiv 1 \pmod{m_k}$$

Logo, a congruência $a_k x \equiv b_k \pmod{m_k}$ é *equivalente* à congruência:

$$x \equiv b_k a_k^* \pmod{m_k}$$

e por conseguinte o sistema dado é *equivalente* ao sistema de congruências lineares:

$$\begin{cases} x \equiv b_1 a_1^* \pmod{m_1} \\ x \equiv b_2 a_2^* \pmod{m_2} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ x \equiv b_r a_r^* \pmod{m_r} \end{cases}$$

o qual tem, pelo "Teorema do resto chinez", uma *única solução módulo* $m = m_1 m_2 \ldots m_r$.

<u>Exemplo 11.4</u> Resolver o sistema de congruências lineares:

$$\begin{cases} 2x \equiv 1 \pmod{5} \\ 3x \equiv 2 \pmod{7} \\ 4x \equiv 3 \pmod{11} \end{cases}$$

Os *módulos* 5, 7 e 11 das congruências do sistema dado são *primos entre si dois a dois* e, além disso:

$$\text{mdc}(2,1) = \text{mdc}(3,2) = \text{mdc}(4,3) = 1$$

de modo que, pelo teorema 11.1, o sistema tem uma *única solução módulo* $m = 5.7.11 = 385$.

As congruências lineares:

$$2x \equiv 1 \pmod{5}, \quad 3x \equiv 1 \pmod{7}, \quad 4x \equiv 1 \pmod{11}$$

tem como *soluções* respectivas: $a_1^* = 3$, $a_2^* = 5$, $a_3^* = 3$, e por conseguinte o sistema dado é *equivalente* ao sistema:

$$\begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 10 \pmod{7} \\ x \equiv 9 \pmod{11} \end{cases}$$

para o qual $X \equiv 108 \pmod{385}$ é a *única solução*.

<u>Exemplo 11.5</u> Resolver a congruência linear:

$$13x \equiv 17 \pmod{42}$$

Por ser $42 = 2.3.7$, a congruência linear dada é *equivalente* ao sistema de congruências lineares:

$$\begin{cases} 13x \equiv 17 \pmod{2} \\ 13x \equiv 17 \pmod{3} \\ 13x \equiv 17 \pmod{7} \end{cases} \quad \text{ou} \quad \begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 4 \pmod{7} \end{cases}$$

A primeira congruência dá-nos $x = 1 + 2a$, onde $\underline{a}$ é um inteiro. Substituindo este valor de $\underline{x}$ na segunda congruência obtemos:

$$1 + 2a \equiv 2 \pmod{3} \Longrightarrow a \equiv 2 \pmod{3}$$

Portanto:

$$a = 2 + 3b \quad e \quad x = 1 + 2(2 + 3b) = 5 + 6b$$

onde b é um inteiro. Substituindo este valor de x na terceira congruência, obtemos:

$$5 + 6b \equiv 4 \pmod{7} \Longrightarrow b \equiv 1 \pmod{7}$$

Portanto:

$$b = 1 + 7c \quad e \quad x = 5 + 6(1 + 7c) = 11 + 42c$$

onde c é um inteiro, e isto significa que

$$x \equiv 11 \pmod{42}$$

é a *única solução* da congruência linear dada

$$13x \equiv 17 \pmod{42}.$$

EXERCÍCIOS

1. Resolver os seguintes sistemas de congruências lineares:

   (a) $x \equiv 1 \pmod{2}$, $x \equiv 1 \pmod{3}$

   (b) $x \equiv 5 \pmod{12}$, $x \equiv 7 \pmod{19}$

   (c) $x \equiv 8 \pmod{26}$, $x \equiv 11 \pmod{33}$

2. Resolver os seguintes sistemas de congruências lineares:

   (a) $x \equiv 3 \pmod{5}$, $x \equiv 5 \pmod{7}$, $x \equiv 7 \pmod{11}$

   (b) $x \equiv 1 \pmod{3}$, $x \equiv 2 \pmod{5}$, $x \equiv 3 \pmod{7}$

   (c) $x \equiv 5 \pmod{6}$, $x \equiv 4 \pmod{11}$, $x \equiv 3 \pmod{17}$

   (d) $x \equiv 5 \pmod{11}$, $x \equiv 14 \pmod{29}$, $x \equiv 15 \pmod{31}$

   (e) $x \equiv 7 \pmod{9}$, $x \equiv 10 \pmod{4}$, $x \equiv 1 \pmod{7}$

   (f) $x \equiv 28 \pmod{29}$, $x \equiv 30 \pmod{31}$, $x \equiv 10 \pmod{11}$

   (g) $x \equiv a \pmod{3}$, $x \equiv b \pmod{5}$, $x \equiv c \pmod{8}$

3. Resolver os seguintes sistemas de congruências lineares:

(a) $$\begin{cases} 5x \equiv 11 \pmod{17} \\ 3x \equiv 19 \pmod{32} \\ 11x \equiv 6 \pmod{37} \end{cases}$$

(b) $$\begin{cases} 2x \equiv 1 \pmod{5} \\ 3x \equiv 9 \pmod{6} \\ 4x \equiv 1 \pmod{7} \\ 5x \equiv 9 \pmod{11} \end{cases}$$

4. Resolver os seguintes sistemas de congruências lineares:

(a) $$\begin{cases} x \equiv 8 \pmod{9} \\ x \equiv 2 \pmod{3} \\ x \equiv 5 \pmod{7} \end{cases}$$

(b) $$\begin{cases} x \equiv 4 \pmod{6} \\ x \equiv 13 \pmod{15} \\ x \equiv 8 \pmod{14} \\ x \equiv 1 \pmod{7} \end{cases}$$

(c) $$\begin{cases} x \equiv 0 \pmod{3} \\ x \equiv 1 \pmod{4} \\ 17x \equiv 9 \pmod{23} \end{cases}$$

CAPÍTULO 12

TEOREMAS DE FERMAT E WILSON

12.1 TEOREMA DE FERMAT

Se p é um primo e se p não divide o inteiro a $(p \nmid a)$, *então:*

$$a^{p-1} \equiv 1 \pmod{p}$$

Demonstração:

Consideremos os p-1 primeiros múltiplos positivos de a, isto é, os inteiros:

$$a,\ 2a,\ 3a,\ \ldots,\ (p-1)a$$

Nenhum desses inteiros é *congruente a* 0 (mod.p), além disso, dois quaisquer deles são *incongruentes* (mod.p), pois, se fosse:

$$ra \equiv sa \pmod{p}, \quad 1 \leqslant r < s \leqslant p-1$$

então, o fator comum a poderia ser *cancelado*, porque o mdc(a,p) = 1, e teríamos:

$$r \equiv s \pmod{p}$$

o que é *impossível*, visto que $0 < s - r < p$.

Assim sendo, cada um dos inteiros a, 2a, 3a,...,(p-1)a é *congruente* (mod.p) a um *único* dos inteiros 1,2,3,...,p-1, considerados numa certa ordem, e por conseguinte multiplicando ordenadamente todas essas p-1 congruências, teremos:

$$a.2a.3a...(p-1)a \equiv 1.2.3...(p-1) \pmod{p}$$

ou seja:

$$a^{p-1}\,(p-1)! \equiv (p-1)! \pmod{p}$$

Como p é *primo* e p *não divide* (p-1)!, podemos *cancelar* o fator comum (p-1)!, o que dá a *congruência de FERMAT:*

$$a^{p-1} \equiv 1 \pmod{p}$$

Corolário 12.1 Se p é um *primo*, então $a^p \equiv a \pmod{p}$, qualquer que seja o inteiro a.

Demonstração:

Se p *divide* a $(p|a)$, então:

$$a \equiv 0 \pmod{p} \quad \text{e} \quad a^p \equiv 0 \pmod{p}$$

o que implica:

$$a^p \equiv a \pmod{p}$$

Se, ao invés, p *não divide* a ($p \nmid a$), então, pelo *teorema de FERMAT:* $a^{p-1} \equiv 1 \pmod{p}$ e, portanto:

$$a.a^{p-1} \equiv a.1 \pmod{p} \quad \text{ou} \quad a^p \equiv a \pmod{p}$$

Exemplo 12.1 Verificar o *teorema de FERMAT* com a = 3 e p = 7.

O inteiro 7 é *primo* e 7 *não divide* 3 ($7 \nmid 3$). Temos:

$$3^{7-1} = 3^6 = 729$$

e como $7 \mid (729 - 1)$, segue-se que $729 \equiv 1 \pmod{7}$, isto é:

$$3^{7-1} \equiv 1 \pmod{7}$$

Exemplo 12.2 Verificar o *teorema de FERMAT* com a = 3 e p = 17.

O inteiro 17 é *primo* e 17 *não divide* 3 ($17 \nmid 3$). Temos:

$$3^{17-1} = 3^{16}$$

mas não é necessário calcular o número muito grande 3^{16}, pois, temos:

$$3^3 = 27 \equiv 10 \pmod{17}$$

o que implica:

$$3^6 \equiv 100 \equiv -2 \pmod{17} \quad e \quad 3^{12} \equiv 4 \pmod{17}$$

Portanto:

$$3^{17-1} = 3^{16} = 3^{12}.3^3.3 \equiv 4.10.3 \equiv 120 \equiv 1 \pmod{17}$$

<u>Exemplo 12.3</u> Mostrar que $5^{38} \equiv 4 \pmod{11}$.

Pelo *teorema de FERMAT:*

$$5^{10} \equiv 1 \pmod{11}$$

o que implica:

$$5^{38} = 5^{10.3+8} = (5^{10})^3(5^2)^4$$

$$\equiv 1^3.3^4 \equiv 81 \equiv 4 \pmod{11}$$

<u>Exemplo 12.4</u> Mostrar que o inteiro 117 é *composto*.

Obviamente, basta achar um inteiro <u>a</u> tal que

$$a^{117} \not\equiv a \pmod{117}$$

Com $a = 2$, temos:

$$2^{117} = 2^{7.16+5} = (2^7)^{16}.2^5$$

Por ser $2^7 = 128 \equiv 11 \pmod{117}$, temos:

$$2^{117} \equiv 11^{16}.2^5 \equiv (121)^8.2^5 \equiv 4^8.2^5 \equiv 2^{21} \pmod{117}$$

Mas, $2^{21} = (2^7)^3$, o que implica:

$$2^{21} \equiv 11^3 \equiv 121.11 \equiv 4.11 \equiv 44 \pmod{117}$$

Portanto:

$$2^{117} \equiv 44 \not\equiv 2 \pmod{117}$$

de modo que o inteiro 117 é *composto* (117 = 9.13).

<u>Teorema 12.1</u> Se <u>p</u> e <u>q</u> são *primos* distintos tais que

$$a^p \equiv a \pmod{q} \quad e \quad a^q \equiv a \pmod{p}$$

então:

$$a^{pq} \equiv a \pmod{pq}$$

<u>Demonstração</u>:

Pelo corolário 12.1, temos:

$$(a^q)^p \equiv a^q \pmod{p} \quad e \quad (a^p)^q \equiv a^p \pmod{q}$$

e, pela hipótese:

$$a^q \equiv a \pmod{p} \quad e \quad a^p \equiv a \pmod{q}$$

o que implica:

$$a^{pq} \equiv a \pmod{p} \quad e \quad a^{pq} \equiv a \pmod{q}$$

ou seja:

$$p|(a^{pq} - a) \quad e \quad q|(a^{pq} - a)$$

E como o $mdc(p,q) = 1$, segue-se que

$$pq|(a^{pq} - a), \text{ isto é: } a^{pq} \equiv a \pmod{pq}$$

<u>Exemplo 12.5</u> Mostrar que $2^{340} \equiv 1 \pmod{341}$.

O inteiro $341 = 11.31$ e $2^{10} = 1024 = 31.33 + 1 =$
$= 11.93 + 1$, o que implica:

$$2^{10} \equiv 1 \pmod{31} \quad e \quad 2^{10} \equiv 1 \pmod{11}$$

Portanto:

$$2^{11} = 2.2^{10} \equiv 2.1 \equiv 2 \pmod{31}$$

$$2^{31} = 2(2^{10})^3 \equiv 2.1^3 \equiv 2 \pmod{11}$$

Os inteiros 11 e 31 são *primos*, de modo que, pelo teorema 12.1, temos:

$$2^{11.31} \equiv 2 \pmod{11.31} \quad ou \quad 2^{341} \equiv 2 \pmod{341}$$

ou seja, *cancelando* o fator comum 2:

$$2^{340} \equiv 1 \pmod{341}$$

Note-se que esta congruência, onde o módulo 341 é *composto*, mostra que o *recíproco* do *teorema de FERMAT*, isto é:

Se $a^{n-1} \equiv 1 \pmod{n}$, então $\underline{n}$ é *primo*, é *falso*.

12.2 TEOREMA DE WILSON

Se $\underline{p}$ *é um primo, então* $(p-1)! \equiv -1 \pmod{p}$.

<u>Demonstração:</u>

O teorema é verdadeiro para $p = 2$ e $p = 3$, pois, temos:

$$(2 - 1)! = 1! = 1 \equiv -1 \pmod{2}$$

$$(3 - 1)! = 2! = 2 \equiv -1 \pmod{3}$$

de modo que vamos supor $p \geqslant 5$.

Consideremos a congruência linear:

$$ax \equiv 1 \pmod{p}$$

onde $\underline{a}$ é um qualquer dos $p-1$ inteiros positivos:

$$1, 2, 3, \ldots, p-1$$

Então, o $mdc(a,p) = 1$ e, pelo corolário 10.1, esta congruência admite uma *única* solução módulo $\underline{p}$, isto é, existe um *único* inteiro a_1, com $1 \leqslant a_1 \leqslant p-1$, tal que $aa_1 \equiv 1 \pmod{p}$.

Como p é *primo*, temos $a = a_1$ se e somente se $a = 1$ ou $a = p-1$.

De fato, a congruência quadrática:

$$a^2 \equiv 1 \pmod{p}$$

é equivalente à seguinte:

$$(a - 1)(a + 1) \equiv 0 \pmod{p}$$

de modo que $p|(a-1)(a+1)$ e, portanto:

$$p|(a - 1) \text{ ou } p|(a + 1),$$

o que implica:

$$a - 1 \equiv 0 \pmod{p} \quad e \quad a = 1$$

$$a + 1 \equiv 0 \pmod{p} \quad e \quad a = p - 1$$

Assim, p.ex. se $p = 13$, temos:

a	1	2	3	4	5	6	7	8	9	10	11	12
a_1	1	7	9	10	8	11	2	5	3	4	6	12

Omitindo os inteiros 1 e $p-1$, com os $p-3$ inteiros restantes: 2, 3, ..., $p-2$, podemos formar $(p-3)/2$ pares a, a_1, com $a \neq a_1$, e tais que

$$aa_1 \equiv 1 \pmod{p}$$

Então, multiplicando ordenadamente todas essas $(p-3)/2$ congruências, obtemos:

$$2.3...(p-2) \equiv 1 \pmod{p}$$

ou

$$(p-2)! \equiv 1 \pmod{p}$$

ou, multiplicando por $p-1$:

$$(p-1)! \equiv p-1 \equiv -1 \pmod{p}$$

Note-se que, com $p = 13$, os 10 inteiros 2,3,...,11 dão lugar a 5 pares tais que o produto dos inteiros de cada par é congruente a 1 (mod.13):

$$2.7 \equiv 1 \pmod{13}$$
$$3.9 \equiv 1 \pmod{13}$$
$$4.10 \equiv 1 \pmod{13}$$
$$5.8 \equiv 1 \pmod{13}$$
$$6.11 \equiv 1 \pmod{13}$$

Multiplicando ordenadamente essas cinco congruências, obtemos:

$$11! = (2.7)(3.9)(4.10)(5.8)(6.11) \equiv 1 \pmod{13}$$

e portanto:

$$12! \equiv 12 \equiv -1 \pmod{13}$$

isto é:

$$(p-1)! \equiv -1 \pmod{p}, \quad \text{com } p = 13$$

O teorema a seguir é o *recíproco* do *teorema de WILSON*.

Teorema 12.1 Se $(n-1)! \equiv -1 \pmod{n}$, então n é *primo*.

Demonstração:

Suponhamos que o inteiro n é *composto*. Então, n tem um divisor d tal que $1 < d < n$. Além disso, como $d \leq n-1$, segue-se que d é um dos fatores de $(n-1)! = 1.2.3....(n-1)$ e, portanto, $d \mid (n-1)!$. Mas, por hipótese, $n \mid (n-1)! + 1$, de modo que $d \mid (n-1)! + 1$. Logo, $d \mid 1$, o que é absurdo. Portanto, n é *primo*.

NOTA. O *teorema de WILSON* e o seu *recíproco* dão um *critério* para se reconhecer se um inteiro dado é *primo:* um inteiro $n > 1$ é *primo* se e somente se

$$(n - 1)! \equiv -1 \pmod{n}.$$

Entretanto, para inteiros grandes este critério é impraticável, e por isso de interesse apenas teórico.

Exemplo 12.6 Verificar o *teorema de WILSON* com $p=7$.

Temos:

$$(7 - 1)! + 1 = 6! + 1 = 720 + 1 = 721 = 7.103$$

Portanto:

$$(7 - 1)! + 1 \equiv 0 \pmod{7}$$

ou

$$(7 - 1)! \equiv -1 \pmod{7}$$

Exemplo 12.7 Reconhecer se o inteiro 11 é *primo*.

Temos:

$$(11-1)! + 1 = 10! + 1 = 1.2.3...10 + 1 =$$
$$= 3628801 = 11.329891$$

e, portanto:

$$(11 - 1)! \equiv -1 \pmod{11}$$

Logo, 11 é *primo*.

EXERCÍCIOS

1. Verificar o teorema de FERMAT com $a = 2$ e $p = 13$.
2. Verificar o teorema de WILSON com $p = 5$.
3. Mostrar que 8 é *composto* usando o teorema de WILSON.
4. Mostrar que 19 é *primo* usando o *recíproco* do teorema de WILSON.
5. Reconhecer se 17 é *primo* usando o teorema de WILSON.
6. Verificar:

   (a) $18^6 \equiv 1 \pmod{49}$ (b) $18^6 \equiv 1 \pmod{343}$

7. Achar o resto da divisão de 15! por 17.

8. Mostrar que, se o mdc(a,35) = 1, então

$$a^{12} \equiv 1 \pmod{35}.$$

9. Demonstrar que, para todo inteiro a, se tem:

(a) $a^{13} \equiv a \pmod{7}$ (b) $a^{37} \equiv a \pmod{13}$

(c) $a^{21} \equiv a \pmod{15}$ (d) $a^{7} \equiv a \pmod{42}$

10. Demonstrar que, para todo inteiro positivo n, se tem:

(a) $2^{2n} \equiv 1 \pmod{3}$ (b) $2^{3n} \equiv 1 \pmod{7}$

11. Mostrar que $18! + 1 \equiv 0 \pmod{437}$.

12. Mostrar:

(a) $561 \mid (2^{561} - 2)$ (b) $561 \mid (3^{561} - 3)$

13. Formar com os inteiros 2,3,4,...,21 todos os *pares* a, b tais que $ab \equiv 1 \pmod{23}$.

CAPÍTULO 13

DIVISORES DE UM INTEIRO

13.1 DIVISORES DE UM INTEIRO

<u>Teorema 13.1</u> Se $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ é a *decomposição canônica* do inteiro positivo $n > 1$, então os *divisores positivos de* <u>*n*</u> são precisamente os inteiros <u>d</u> da forma:

$$d = p_1^{h_1} p_2^{h_2} \ldots p_r^{h_r}$$

onde $0 \leq h_i \leq k_i$ $(i = 1,2,\ldots,r)$.

<u>Demonstração:</u>

Obviamente, os *divisores triviais* $d = 1$ e $d = n$ de <u>n</u> se obtem quando, respectivamente:

$$h_1 = h_2 = \ldots = h_r = 0$$

e

$$h_1 = k_1, \quad h_2 = k_2, \ldots, \quad h_r = k_r$$

Suponhamos, pois, que $\underline{d}$ é um *divisor não trivial* de $\underline{n}$, isto é:

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

Exprimindo $\underline{d}$ e d_1 como produtos de (não necessariamente distintos) *primos:*

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

obtemos:

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} = q_1 q_2 \cdots q_s t_1 t_2 \cdots t_u$$

que são *duas decomposições* do inteiro positivo $\underline{n}$ num produto de *primos*, e como é *única* uma decomposição de $\underline{n}$ de tal natureza, então cada primo q_i *coincide* com um p_j, de modo que, substituindo os produtos de primos iguais por potências de expoente inteiro, teremos:

$$d = q_1 q_2 \cdots q_s = p_1^{h_1} p_2^{h_2} \cdots p_r^{h_r}$$

onde é possível algum $h_i = 0$.

Reciprocamente, todo inteiro

$$d = p_1^{h_1} p_2^{h_2} \cdots p_r^{h_r} \quad (0 \leqslant h_i \leqslant k_i)$$

é um *divisor* de $\underline{n}$, pois, podemos escrever:

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} = (p_1^{h_1} p_2^{h_2} \cdots p_r^{h_r})(p_1^{k_1-h_1} p_2^{k_2-h_2} \cdots p_r^{k_r-h_r}) =$$

$$= d(p_1^{k_1-h_1} p_2^{k_2-h_2} \cdots p_r^{k_r-h_r})$$

onde $k_i - h_i \geq 0$ para cada $\underline{i}$. Logo, $\underline{d}$ é um *divisor* de $\underline{n}$ $(d|n)$.

<u>Exemplo 13.1</u> Os *divisores positivos* do inteiro

$$n = 1350 = 2.3^3.5^2$$

são precisamente os inteiros $\underline{d}$ da forma:

$$d = 2^{h_1}.3^{h_2}.5^{h_3}$$

onde

$$0 \leqslant h_1 \leqslant 1, \quad 0 \leqslant h_2 \leqslant 3, \quad 0 \leqslant h_3 \leqslant 2$$

isto é:

$$h_1 = 0,1, \quad h_2 = 0,1,2,3, \quad h_3 = 0,1,2$$

Assim, com $h_1 = 1$, $h_2 = 2$ e $h_3 = 0$, obtemos o *divisor:*

$$d = 2.3^2.5^0 = 2.9.1 = 18$$

do inteiro 1350. Realmente: $1350 = 18.75$.

Com $h_1 = h_2 = h_3 = 0$ e $h_1 = 1$, $h_2 = 3$, $h_3 = -2$ acham-se os *divisores triviais* $d = 1$ e $d = 1350$ do inteiro dado 1350.

13.2 NÚMERO DE DIVISORES

Seja n um inteiro positivo. O *número de divisores positivos* de n (inclusive 1 e n) indica-se por d(n).

Assim, p.ex., os *divisores positivos* de 12 são 1,2,3,4,4, 6 e 12, de modo que d(12) = 6.

Se p é um *primo*, então d(p) = 2, porque os únicos *divisores positivos* de p são 1 e p. E como os *divisores positivos* de p^2 são 1, p e p^2, temos $d(p^2) = 3$. De modo geral, $d(p^n) = n + 1$, porque os *divisores positivos* de p^n são $1, p, p^2, \ldots, p^n$.

A tabela abaixo dá o *número de divisores positivos* dos inteiros de 1 até 10:

n	1	2	3	4	5	6	7	8	9	10
d(n)	1	2	2	3	2	4	2	4	3	4

Teorema 13.2 Se $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ é a *decomposição canônica* do inteiro positivo $n > 1$, então:

$$d(n) = (k_1 + 1)(k_2 + 1)\ldots(k_r + 1)$$

Demonstração:

Consoante o teorema 13.1, os *divisores positivos* de $\underline{n}$ são precisamente os inteiros $\underline{d}$ da forma:

$$d = p_1^{h_1} p_2^{h_2} \cdots p_r^{h_r}$$

onde

$$0 \leqslant h_1 \leqslant k_1, \quad 0 \leqslant h_2 \leqslant k_2, \quad \ldots, \quad 0 \leqslant h_r \leqslant k_r$$

Temos $k+1$ maneiras de escolher o expoente h_1, k_2+1 maneiras de escolher o expoente $h_2, \ldots, k_r+1$ maneiras de escolher o expoente h_r e, portanto, o número total de maneiras de escolher os expoentes $h_1, h_2, \ldots, h_r$ é dado pelo produto:

$$(k_1 + 1)(k_2 + 1) \ldots (k_r + 1)$$

Assim sendo, o número $d(n)$ de *divisores positivos* do inteiro $n > 1$ é dado pela fórmula:

$$d(n) = (k_1 + 1)(k_2 + 1) \ldots (k_r + 1)$$

ou seja:

$$d(n) = \prod_{i=1}^{r} (k_i + 1)$$

Note-se que

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

<u>Exemplo 13.2</u> O *número de divisores positivos* do inteiro

$$n = 756 = 2^2.3^3.7$$

é:

$$d(756) = (2 + 1)(3 + 1)(1 + 1) = 3.4.2 = 24$$

Estes 24 *divisores positivos* de 756 são os inteiros $\underline{d}$ da forma:

$$d = 2^{h_1}3^{h_2}7^{h_3}$$

onde $h_1 = 0,1,2$, $h_2 = 0,1,2,3$ e $h_3 = 0,1$.

O cálculo para a determinação efetiva destes 24 *divisores positivos* de 756 pode dispor-se do seguinte modo:

	1	2	4
3	3	6	12
9	9	18	36
27	27	54	108
7	7	14	28
	21	42	84
	63	126	252
	189	378	756

Na primeira linha, do lado direito, escrevem-se as potências do primeiro fator primo 2, isto é: 1,2 e 4. Na segunda, terceira e quarta linhas, do lado esquerdo, escrevem-

se, por baixo uma das outras, as diversas potências do segundo fator primo 3, a partir da primeira potência, no caso presente 3, 9 e 27, e à direita de cada uma delas escrevem-se os produtos dessa potência por todos os inteiros da primeira linha. A seguir, do lado esquerdo, escrevem-se as potências do terceiro fator primo 7, a partir da primeira (no caso 7), e à direita escrevem-se os produtos dessas potências por todos os inteiros que do lado direito figuram nas linhas anteriores. Se houvesse mais fatores primos procedia-se com eles como para o caso do terceiro fator primo.

Exemplo 13.3 Achar o *menor* inteiro positivo n que tem 10 divisores positivos.

Como $10 = 10.1 = 5.2$, temos:

$$d(n) = (k_1 + 1)(k_2 + 2) = 10.1$$

ou

$$d(n) = (k_1 + 1)(k_2 + 2) = 5.2$$

Portanto, os expoentes, k_1 e k_2 dos fatores primos de n são 9 e 0, ou 4 e 1. E como $2^4.3$ é menor que 2^9, o *menor* inteiro positivo com 10 divisores positivos é $2^4.3 = 48$.

Exemplo 13.4 Achar o inteiro positivo da forma 9.10^m e que admite 27 divisores positivos.

Por ser $9.10^m = 3^2.2^m.5^m$, devemos ter:

$$(2 + 1)(m + 1)(m + 1) = 27$$

ou

$$(m + 1)^2 = 9 \Longrightarrow m + 1 = 3 \quad e \quad m = 2$$

Logo, o inteiro positivo procurado é $9.10^2 = 900$.

13.3 SOMA DE DIVISORES

Seja n um inteiro positivo. A *soma dos divisores positivos* de n (inclusive 1 e n) indica-se por $s(n)$.

Assim, p.ex., os *divisores positivos* de 12 são 1,2,3,4,6 e 12, de modo que

$$s(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28$$

Se p é um *primo*, então $s(p) = 1 + p$, porque os únicos divisores positivos de p são 1 e p. E como os *divisores positivos* de p^2 são 1, p e p^2, temos:

$$s(p^2) = 1 + p + p^2 = \frac{p^3 - 1}{p - 1}$$

De modo geral, os *divisores positivos* de p^n são

$$1, p, p^2, \ldots, p^n$$

e, portanto:

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

Em particular:

$$s(2^n) = 2^{n+1} - 1 \quad \text{e} \quad s(3^n) = \frac{1}{2}(3^{n+1} - 1)$$

A tabela abaixo dá a *soma dos divisores positivos* dos inteiros de 1 até 10:

n	1	2	3	4	5	6	7	8	9	10
s(n)	1	3	4	7	6	12	8	15	13	18

<u>Teorema 13.3</u> Se

$$n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$$

é a *decomposição canônica* do inteiro positivo $n > 1$, então

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

<u>Demonstração</u>:

Consideremos o produto:

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

$$(1 + p_r + p_r^2 + \ldots + p_r^{k_r}).$$

Pelo teorema 13.1, cada divisor positivo de $\underline{n}$ é um termo do desenvolvimento deste produto e vice-versa, de modo que

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

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

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

ou seja:

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

Note-se que

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

<u>Exemplo 13.5</u> A *soma dos divisores positivos* do inteiro

$$n = 180 = 2^2 . 3^2 . 5$$

é:

$$s(180) = \frac{2^3 - 1}{2 - 1} \cdot \frac{3^3 - 1}{3 - 1} \cdot \frac{5^2 - 1}{5 - 1} = 7.13.6 = 546$$

Realmente, os *divisores positivos* de 180 são:

1,2,3,4,5,6,9,10,12,15,18,20,30,36,45,60,90,180

e a soma destes 18 divisores é 546.

13.4 NOTAÇÃO

Seja n um inteiro positivo. Com o símbolo

$$\sum_{d|n} f(d)$$

indica-se a *soma* dos valores de f(d) quando d é sucessivamente igual a cada um dos *divisores positivos* de n. Assim, p.ex.:

$$\sum_{d|20} f(d) = f(1) + f(2) + f(4) + f(5) + f(10) + f(20)$$

$$\sum_{d|10} d^2 = 1^2 + 2^2 + 5^2 + 10^2 = 1 + 4 + 25 + 100 = 130$$

Com esta notação, temos:

$$d(n) = \sum_{d|n} 1 \quad \text{e} \quad s(n) = \sum_{d|n} d$$

Assim, p.ex.:

$$d(10) = \sum_{d|10} 1 = 1 + 1 + 1 + 1 = 4$$

$$s(10) = \sum_{d|10} d = 1 + 2 + 5 + 10 = 18$$

Analogamente, o *produto* dos valores de f(d) quando d é sucessivamente igual a cada um dos *divisores positivos* de n indica-se pelo símbolo:

$$\prod_{d|n} f(d)$$

Assim, p.ex.:

$$\prod_{d|12} f(d) = f(1)f(2)f(3)f(4)f(6)f(12)$$

$$\prod_{d|20} d = 1.2.4.5.10.20 = 8000$$

13.5 PRODUTO DE DIVISORES

Teorema 13.4 O produto dos divisores positivos de um inteiro positivo $n > 1$ é igual a $n^{d(n)/2}$.

Demonstração:

Sejam $d_1, d_2, \ldots, d_k$ *todos* os divisores positivos de $\underline{n}$, de modo que existem os inteiros $q_1, q_2, \ldots, q_k$ tais que

$$n = d_1 q_1, \quad n = d_2 q_2, \quad \ldots, \quad n = d_k q_k$$

Multiplicando ordenadamente todas essas $\underline{k}$ igualdades, obtemos:

$$n^k = (d_1 d_2 \ldots d_k)(q_1 q_2 \ldots q_k)$$

Como $d_1 d_2 \ldots d_k = q_1 q_2 \ldots q_k$, porque cada um dos inteiros $q_1, q_2, \ldots, q_k$ também é um *divisor* de $\underline{n}$, temos:

$$n^{d(n)} = (d_1 d_2 \ldots d_k)^2$$

donde

$$d_1 d_2 \ldots d_k = n^{d(n)/2}$$

ou seja:

$$\prod_{d|n} d = n^{d(n)/2}$$

Exemplo 13.6 O *produto dos divisores positivos* do inteiro $n = 16$ é:

$$\prod_{d|16} d = 16^{d(16)/2} = 16^{5/2} = (4^2)^{5/2} = 4^5 = 1024$$

Realmente, os *divisores positivos* de 16 são 1,2,4,8,16 e o produto destes 5 divisores é igual a 1024.

EXERCÍCIOS

1. Sendo p e q *primos*, calcular: $d(pq)$, $d(p^2q)$ e $d(p^3q)$.

2. Calcular: $d(42)$, $d(240)$, $d(420)$ e $d(10115)$.

3. Achar o número de divisores positivos de cada um dos seguintes inteiros:
   (a) 144; (b) 360; (c) 1009; (d) 6534.

4. Achar o número de divisores positivos do produto 9.24.42.

5. Achar o *menor* inteiro positivo com *seis* divisores positivos.

6. Achar o *menor* inteiro positivo n tal que $d(n) = 8$.

7. Achar o inteiro positivo da forma 28.15^m e que admite 54 divisores positivos.

8. Achar o inteiro positivo da forma $2.15^m.7^n$ e que admite 36 divisores positivos.

9. Sendo p e q *primos*, calcular:
   $s(pq)$, $s(p^3)$ e $s(p^2q)$.

10. Calcular:

    $s(240)$, $s(420)$, $s(1008)$ e $s(10115)$.

11. Achar a soma dos divisores positivos de cada um dos seguintes inteiros:

(a) 144; (b) 360; (c) 1009; (d) 6534.

12. Calcular:

$d(s(360))$ e $s(d(180))$.

13. Verificar que $s(n) = 2n$ para $n = 6, 28, 496, 8128$.

14. Verificar que $s(n) = 3n$ para $n = 120$ e $n = 672$.

15. Verificar que $s(n) = s(n+1)$ para $n = 957$ e $n = 14206$.

16. Verificar as seguintes relações:

(a) $s(8)s(3) = s(24)$

(b) $s(8)s(9) = s(72)$

(c) $s(4)s(27) = s(108)$

17. Verificar que

$$d(n) = d(n+1) = d(n+2) = d(n+3)$$

para $n = 3655$ e $n = 4503$.

18. Achar os inteiros positivos menores que 10000 e com 60 divisores positivos.

19. Achar todos os *primos* com 90 que dividem o produto 90.1274.

20. Achar todos os inteiros positivos tais que na divisão de 167 por cada um deles se obtenha o mesmo *resto* 17.

21. Determinar o inteiro $n = 2^x.3^y$, sabendo que $n/6$ e $n/9$ têm, respectivamente, 8 divisores positivos e 10 divisores positivos a menos que n.

22. Determinar o inteiro $n = 2^x.5^y.7^z$, sabendo que os produtos 5n, 7n e 8n têm, respectivamente, 8,12,e 18 divisores positivos a mais que n.

23. Resolver as equações:

    (a) $s(x) = 36$;

    (b) $s(x) = 60$.

24. Mostrar que não existe inteiro positivo n tal que $s(n) = 10$.

25. Demonstrar:

    (a) $d(n) \leqslant 2\sqrt{n}$;

    (b) $n \leqslant s(n) \leqslant n^2$.

CAPÍTULO 14

FUNÇÕES ARITMÉTICAS

14.1 CONCEITO DE FUNÇÃO ARITMÉTICA

Definição 14.1 Chama-se *função aritmética* toda função f *definida* no conjunto N dos inteiros positivos e com *valores* no conjunto Z dos inteiros, isto é, toda função f de N em Z($f: N \to Z$).

Portanto, o *domínio* e o *contradomínio* de uma *função aritmética* f são os conjuntos N e Z, respectivamente, e a *imagem* é o conjunto:

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

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

Duas *funções aritméticas* importantes são as funções d e s de N em N($d,s: N \to N$) assim definidas para todo inteiro positivo n:

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

$s(n)$ = soma dos divisores positivos de $\underline{n}$

14.2 FUNÇÕES ARITMÉTICAS MULTIPLICATIVAS

Definição 14.2 Uma função aritmética f diz-se uma *função aritmética multiplicativa* se

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

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

Assim, p.ex., são *funções aritméticas multiplicativas* as funções $\underline{f}$ e $\underline{g}$ definidas por $f(n) = 1$ (função constante) e $g(n) = n$ para todo inteiro positivo $\underline{n}$, pois, quaisquer que sejam os inteiros positivos $\underline{r}$ e $\underline{s}$, temos:

$$f(rs) = 1 = 1.1 = f(r)f(s)$$
$$g(rs) = rs = g(r)g(s)$$

Note-se que, para estas duas funções, f e g, se verifica a igualdade $f(rs) = f(r)f(s)$ mesmo sem a condição de o $mdc(r,s) = 1$.

Se $\underline{f}$ é uma *função aritmética multiplicativa* e se $n_1, n_2, \ldots, n_k$ são inteiros positivos *primos entre si dois a dois*, entao, usando o "Teorema da indução matemática" conclui-se:

$$f(n_1,n_2\ldots n_k) = f(n_1)f(n_2)\ldots f(n_k)$$

Portanto, se $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ é a *decomposição canônica* de um inteiro positivo $n > 1$, como os fatores

$$p_i^{k_i}$$

são *primos entre si dois a dois*, temos:

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

Esta igualdade mostra que uma *função aritmética multiplicativa* fica completamente determinada quando os seus valores para potências de *primos* são conhecidos.

Importa ainda notar que, para toda *função aritmética multiplicativa* não identicamente nula se tem $f(1) = 1$, pois existe necessariamente um inteiro positivo $\underline{r}$ tal que $f(r) \neq 0$ e como o $mdc(r,1) = 1$, temos:

$$f(r) = f(r.1) = f(r)f(1) \Longrightarrow f(1) = 1$$

<u>Teorema 14.1</u> As funções $d(n)$ e $s(n)$ são ambas *funções aritméticas multiplicativas.*

<u>Demonstração:</u>

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

$$d(uv) = d(u)d(v) \quad e \quad s(uv) = s(u)s(v)$$

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

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

as *decomposições canônicas* de $\underline{u}$ e $\underline{v}$.

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

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

e, portanto:

$$d(uv) = \left[(k_1 + 1)\ldots(k_i + 1) \right] \left[(h_i + 1)\ldots(h_j + 1) \right] =$$

$$= d(u)d(v)$$

e

$$s(uv) = \left[\frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdots \frac{p_i^{k_i+1} - 1}{p_i - 1} \right] \left[\frac{q_1^{h_1+1} - 1}{q_1 - 1} \cdots \frac{q_j^{h_j+1} - 1}{q_j - 1} \right] =$$

$$= s(u)s(v)$$

de modo que $d(n)$ e $s(n)$ são *funções aritméticas multiplicativas*.

Exemplo 14.1 Verificar que a função d(n) é uma *função aritmérica multiplicativa* para n = 144.

Temos $144 = 2^4.3^2$ e o mdc(16,9) = 1. Portanto:

$$d(144) = (4 + 1)(2 + 1) = 5.3 = 15$$

$$d(16) = 4 + 1 = 5$$

$$d(9) = 2 + 1 = 3$$

isto é:

$$d(144) = d(16)d(9)$$

Exemplo 14.2 Verificar que a função s(n) é uma *função aritmética multiplicativa* para n = 63.

Temos $63 = 3^2.7$ e o mdc(9,7) = 1. Portanto:

$$s(63) = \frac{3^3 - 1}{3-1} \cdot \frac{7^2 - 1}{7-1} = 13.8 = 104$$

$$s(9) = \frac{3^3 - 1}{3 - 1} = 13$$

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

isto é:

$$s(63) = s(9)s(7)$$

Teorema 14.2 Se f é uma *função aritmética multiplicativa* e se g é a *função aritmética* assim definida:

$$g(n) = \sum_{d|n} f(d)$$

então g também é uma *função aritmética multiplicativa.*

Demonstração:

Sejam r e s dois inteiros positivos tais que o mdc(r,s)=1. Como o conjunto dos divisores positivos de rs consiste de todos os produtos xy, onde $x|r$, $y|s$ e o mdc(x,y) = 1, temos:

$$g(rs) = \sum_{d|rs} f(d) = \sum_{x|r,y|s} f(xy)$$

Pela definição de *função aritmética multiplicativa:*

$$f(xy) = f(x)f(y)$$

e, portanto:

$$g(rs) = \sum_{x|r,y|s} f(x)f(y) = \left(\sum_{x|r} f(x)\right)\left(\sum_{y|s} f(y)\right) =$$

$$= g(r)g(s)$$

isto é, a *função aritmética* g é *multiplicativa.*

Exemplo 14.3 Verificar que a *função aritmética* g(n) é *multiplicativa* para n = 24.

Temos 24 = 3.8 e o mdc(3,8) = 1. Portanto:

$$g(3.8) = \sum_{d|24} f(d) =$$

$$= f(1) + f(2) + f(3) + f(4) + f(6) + f(8) + f(12) + f(24)$$

ou seja:

$$g(3.8) = f(1.1) + f(1.2) + f(1.3) + f(1.4) + f(2.3) + f(1.8) + f(3.4) + f(3.8) =$$

$$= f(1)f(1) + f(1)f(2) + f(1)f(3) + f(1)f(4) + f(2)f(3) + f(1)f(8) + f(3)f(4) + f(3)f(8)$$

isto é:

$$f(3.8) = \left[f(1) + f(3)\right]\left[f(1) + f(2) + f(4) + f(8)\right] =$$

$$= \sum_{d|3} f(d) \cdot \sum_{d|8} f(d) = g(3)g(8)$$

14.3 FUNÇÃO DE MOBIUS

Definição 14.3 Chama-se *função de MOBIUS* a *função aritmética* u assim definida:

$$u(n) = \begin{cases} 1 & \text{se } n = 1 \\ 0 & \text{se } p^2 | n, \text{ sendo } \underline{p} \text{ um } \textit{primo} \\ (-1)^r & \text{se } n = p_1 p_2 \ldots p_r \text{ onde} \\ & \text{os } p_i \text{ são } \textit{primos} \text{ distintos} \end{cases}$$

Assim, p.ex.:

$$u(6) = u(2.3) = (-1)^2 = 1$$

$$u(12) = u(2^2.3) = 0$$

$$u(42) = u(2.3.7) = (-1)^3 = -1$$

$$u(250) = u(2.5^3) = 0$$

Note-se que, se $\underline{p}$ é um *primo*, então:

$$u(p) = -1 \quad \text{e} \quad u(p^k) - 0 \quad \text{para} \quad k \geqslant 2$$

A tabela abaixo dá os valores de u(n) para os dez primeiros inteiros positivos:

n	1	2	3	4	5	6	7	8	9	10
u(n)	1	-1	-1	0	-1	1	-1	0	0	1

<u>Teorema 14.3</u> A *função* $\underline{u}$ *de MOBIUS* é uma *função aritmética multiplicativa.*

<u>Demonstração:</u>

Sejam $\underline{r}$ e $\underline{s}$ dois inteiros positivos tais que o mdc(r,s)=1.

Cumpre demonstrar que $u(rs) = u(r)u(s)$.

Se $r = 1$, então:

$$u(rs) = u(s) = 1.u(s) = u(1)u(s) = u(r)u(s)$$

Analogamente, se $s = 1$, então $u(rs) = u(r)u(s)$.

Suponhamos, agora, $r > 1$ e $s > 1$. Se $p^2 | r$ ou $p^2 | s$, sendo p um *primo*, então $p^2 | rs$, e temos: $u(rs) = 0 = u(r)u(s)$.

Se, ao invés, $\underline{r}$ e $\underline{s}$ não são divisíveis pelo quadrado de qualquer *primo*, então:

$$r = p_1 p_2 \cdots p_m \quad e \quad s = q_1 q_2 \cdots q_n$$

onde os *primos* p_i e q_j são todos *distintos*, e temos:

$$\begin{aligned} u(rs) &= u(p_1 p_2 \cdots p_m q_1 q_2 \cdots q_n) = \\ &= (-1)^{m+n} = (-1)^m (-1)^n = u(r)u(s) \end{aligned}$$

o que completa a demonstração do teorema.

<u>Teorema 14.4</u> Se $\underline{n}$ é um inteiro positivo, então:

$$\sum_{d|n} u(d) = \begin{cases} 1 & \text{se } n = 1 \\ 0 & \text{se } n > 1 \end{cases}$$

<u>Demonstração</u>:

Consideremos a *função aritmética* $\underline{g}$ assim definida:

$$g(n) = \sum_{d|n} u(d)$$

Se $n = 1$, então:

$$g(1) = \sum_{d|1} u(d) = u(1) = 1$$

Suponhamos, agora, $n > 1$. Se $n = p^k$, sendo $\underline{p}$ um *primo* e $k \geqslant 1$ um inteiro, então os divisores positivos de p^k são os $k+1$ inteiros: $1, p, p^2, \ldots, p^k$, e temos:

$$g(p^k) = \sum_{d|p^k} u(d) = u(1) + u(p) + u(p^2) + \ldots + u(p^k)$$

ou seja:

$$g(p^k) = \sum_{d|p^k} u(d) = u(1) + u(p) = 1 + (-1) = 0$$

Finalmente, se $n = p_1^{k_1} p_2^{k_2} \ldots p_i^{k_i}$ é a *decomposição canônica* de $\underline{n}$, como a *função* $\underline{u}$ *de* MOBIUS é *multiplicativa* (Teorema 14.3), então a *função aritmética* $\underline{g}$ também é *multiplicativa* (Teorema 14.2), e temos:

$$g(n) = g(p_1^{k_1}) g(p_2^{k_2}) \ldots g(p_i^{k_i}) = 0$$

Suponhamos, p.ex., $n = 10$. Como os divisores positivos de 10 são 1, 2, 5 e 10, temos:

$$\sum_{d|10} u(d) = u(1) + u(2) + u(5) + u(10) =$$

$$= 1 + (-1) + (-1) + 1 = 0$$

14.4 FUNÇÕES ARITMÉTICAS MULTIPLICATIVAS COMPLETAS

Definição 14.4 Uma função aritmética $f: N \to Z$ diz-se uma *função aritmética multiplicativa completa* se $f(rs) = f(r)f(s)$ para todo par de inteiros positivos r e s.

Assim, p.ex., a função aritmética f definida por $f(n) = n^3$ é uma *função aritmética multiplicativa completa*, pois, quaisquer que sejam os inteiros positivos r e s, temos:

$$f(rs) = (rs)^3 = r^3s^3 = f(r)f(s)$$

As funções aritmética $d(n)$, $s(n)$ e $u(n)$ *não são funções aritméticas multiplicativas completas*, pois, temos:

$$d(2.10) = d(20) = 6 \neq 2.4 = d(2).d(10)$$

$$s(2.10) = s(20) = 42 \neq 2.18 = s(2).s(10)$$

$$u(2.10) = u(20) = 0 \neq (-1).1 = u(2).u(10)$$

14.5 FUNÇAO MAIOR INTEIRO

Definição 14.5 Para todo número *real* x indica-se por $[x]$ o *maior inteiro que não supera* x, isto é, $[x]$ é o *único* inteiro que satisfaz à condição: $x - 1 < [x] \leq x$.

Assim, p.ex.:

$$[-3/2] = -2, \quad [\sqrt{2}] = 1 \quad , \quad [1/3] = 0$$

$$[\pi] = 3 \quad , \quad [-\pi] = -4, \quad \text{etc.}$$

Importa notar que se tem a igualdade $[x] = x$ se e somente se $\underline{x}$ é um inteiro, e que todo número real $\underline{x}$ pode escrever-se sob a forma:

$$x = [x] + k \ , \quad \text{onde} \quad 0 \leqslant k < 1$$

A função $f: R \to R$ definida por $f(x) = [x]$ chama-se *"função maior inteiro"*. Não é uma função aritmética, porque o seu *domínio* é o conjunto $R \neq N$ dos números reais, mas desempenha papel importante no tratamento dos problemas de divisibilidade.

Observe-se que

$$\sum_{d|n} u(d) = \left[1/n \right]$$

onde $\underline{u}$ é a *função de MOBIUS*.

A *"função maior inteiro"* também é denominada *"função colchête"* ou *"função escada"* (por virtude do seu gráfico cartesiano).

Também se costuma consideraraa função $\{x\} = x - [x]$, denominada *parte fracionária de* $\underline{x}$.

Assim, p.ex.:

$$\{7\} = 0, \quad \{2,6\} = 0,6, \quad \{-4,75\} = 0,25$$

14.6 FÓRMULA DE INVERSÃO DE MOBIUS

Teorema 14.5 Sejam f e g duas *funções aritméticas* relacionadas pela igualdade:

$$f(n) = \sum_{d|n} g(d)$$

Então:

$$g(n) = \sum_{d|n} u(d)f(n/d)$$

Demonstração:

Obviamente, temos:

$$\sum_{d|n} u(d)f(n/d) = \sum_{d|n} \left(u(d) \sum_{c|(n/d)} g(c) \right) =$$

$$= \sum_{d|n} \left(\sum_{c|(n/d)} u(d)g(c) \right)$$

A última soma dupla é sobre todos os pares de inteiros positivos (c,d) tais que $d|n$ e $c|(n/d)$. E como $d|n$ e $c|(n/d)$ se e somente se $c|n$ e $d|(n/c)$, temos:

$$\sum_{d|n}\left(\sum_{c|(n/d)} u(d)g(c)\right) = \sum_{c|n}\left(\sum_{d|(n/c)} u(d)g(c)\right) =$$

$$= \sum_{c|n}\left(g(c) \sum_{d|(n/c)} u(d)\right)$$

Consoante o teorema 14.4, a soma

$$\sum_{d|(n/c)} u(d)$$

tem o valor 0 se $n/c > 1$ e tem o valor 1 se $n/c = 1$ ou $n = c$. Assim sendo, temos, finalmente:

$$\sum_{d|n} u(d)f(n/d) = \sum_{c=n} g(c).1 = g(n)$$

Note-se que

$$\sum_{d|n} u(d)f(n/d) = \sum_{d|n} u(n/d)f(d) = g(n)$$

Assim, p.ex., no caso das funções aritméticas $d(n)$ e $s(n)$ temos, por definição:

$$d(n) = \sum_{e|n} 1 \quad \text{e} \quad s(n) = \sum_{d|n} d$$

e, portanto, pela *fórmula de inversão de* MOBIUS:

$$1 = \sum_{e|n} u(e)d(n/e) = \sum_{e|n} u(n/e)d(e)$$

$$n = \sum_{d|n} u(d)s(n/d) = \sum_{d|n} u(n/d)s(d)$$

fórmulas válidas para todo $n \geq 1$.

EXERCÍCIOS

1. Mostrar que é *multiplicativa* a função aritmética $f(n) = n^k$, onde $\underline{k}$ é um inteiro fixo positivo.

2. Mostrar que, se $f(n)$ e $g(n)$ são *funções aritméticas multiplicativas*, então a *função aritmética*

$$h(n) = f(n)g(n)$$

também é *multiplicativa*.

3. Mostrar que, se $f(n)$ e $g(n)$ são *funções aritméticas multiplicativas* tais que $f(p^k) = g(p^k)$ para todo $\underline{p}$ *primo* e $k \geq 1$, então $f = g$.

4. Sendo $\underline{u}$ a *função de MOBIUS*, demonstrar:

   (a) $u(n)u(n+1)u(n+2)u(n+3) = 0, \quad \forall\, n \geq 1$

   (b) $u(1!) + u(2!) + \ldots + u(n!) = 1, \quad \forall\, n \geq 3$

5. Resolver as duas seguintes equações:

(a) $[x + 3] = x + 3$

(b) $[x + 3] = 3 + [x]$

6. Resolver a equação:

$$[x] + [x] = [2x].$$

7. Sejam $\underline{x}$ e $\underline{y}$ números reais. Demonstrar as seguintes propriedades da *"função maior inteiro"*:

(a) $[x + n] = [x] + n, \forall n \in Z$

(b) $[x] + [-x] = 0$ ou 1, consoante $x \in Z$ ou $x \notin Z$

(c) $[x] + [y] \leqslant [x + y] \leqslant [x] + [y] + 1$

(d) $[x]\,[y] \leqslant [xy]$

CAPÍTULO 15

FUNÇÃO E TEOREMA DE EULER

15.1 FUNÇÃO DE EULER

Definição 15.1 Chama-se *função de EULER* a função aritmética ϕ(fi) assim definida para todo inteiro positivo n:

$\phi(n)$ = número de inteiros positivos que não *superam* n e que são *primos* com n.

Em outros termos: $\phi(n)$ = número de elementos do conjunto

$$\{x \in N \mid 1 \leq x \leq n \quad e \quad mdc(x,n) = 1\}$$

Em particular, $\phi(1) = 1$, porque o $mdc(1,1) = 1$, e para $n > 1$, o $mdc(n,n) = n \neq 1$, de modo que $\phi(n)$ = número de inteiros positivos *menores* que n e *primos* com n.

Esta importante função aritmética $\phi(n)$ também é denominada o *indicador de* n e, menos frequentemente, o *totalizador de* n.

Exemplo 15.1 Se $n = 30$, então os inteiros positivos *menores* que 30 e *primos* com 30 são 1,7,11,13,17,19,23 e 29, de modo que $\phi(30) = 8$.

Exemplo 15.2 Se $n = 12$, então o conjunto

$$\{ x \in N \mid 1 \leqslant x \leqslant 12 \text{ e } mdc(x,12)\} =$$

$$= \{ 1,5,7,11 \}$$

tem 4 elementos, de modo que $\phi(12) = 4$.

Exemplo 15.3 Calcular: $d(\phi(15))$ e $\phi(d(15))$

Temos:

$$d(\phi(15)) = d(8) = 4$$

$$\phi(d(15)) = \phi(4) = 2$$

A tabela abaixo dá os valores de $\phi(n)$ para os dez primeiros inteiros positivos:

n	1	2	3	4	5	6	7	8	9	10
$\phi(n)$	1	1	2	2	4	2	6	4	6	4

Teorema 15.1 A função ϕ de EULER é uma *função aritmética multiplicativa.*

Demonstração:

Demonstração:

Sejam r e s dois inteiros positivos tais que o mdc(r,s)=1. Cumpre demonstrar que $\phi(rs) = \phi(r)\,\phi(s)$.

A proposição é verdadeira se r ou s é igual a 1, pois, temos:

$$(1.s) = \phi(s) = 1.\phi(s) = \phi(1)\ \phi(s)$$

$$(r.1) = \phi(r) = \phi(r).1 = \phi(r)\ \phi(1)$$

Suponhamos, pois, $r > 1$ e $s > 1$. Neste caso os inteiros de 1 a rs podem ser dispostos em r *colunas* com s inteiros em cada uma delas, do seguinte modo:

1	2	. . .	h	...	r
r + 1	r + 2		r + h		2r
2r + 1	2r + 2		2r + h		3r
⋮	⋮		⋮		⋮
(s-1)r + 1	(s-1)r + 2		(s-1)r+h		sr

Por ser o mdc(qr + h,r) = mdc(h,r), os inteiros da h-ésima coluna são *primos* com r se e somente se h é *primo* com r. E como na primeira linha o número de inteiros que são *primos* com r é igual a $\phi(r)$, segue-se que existem somente $\phi(r)$ colunas formadas com inteiros que são todos *primos* com r. Por outro lado, em cada uma destas $\phi(r)$ colunas

existem precisamente $\phi(s)$ inteiros que são *primos* com $\underline{s}$, porque na progressão aritmética:

$$h,\ r+h,\ 2r+h,\ \ldots,\ (s-1)r+h$$

onde o $mdc(h,r) = 1$, o número de termos que são *primos* com $\underline{s}$ é igual a $\phi(s)$. Assim sendo, o número total de inteiros que são *primos* com $\underline{r}$ e com $\underline{s}$, isto é, que são *primos* com $\underline{rs}$, é igual a $\phi(r)\ \phi(s)$, e isto significa que $\phi(rs) = \phi(r)\ \phi(s)$.

15.2 CÁLCULO DE $\phi(n)$

<u>Teorema 15.2</u> Se o inteiro $n > 1$, então $\phi(n) = n - 1$ se e somente se $\underline{n}$ é *primo*.

<u>Demonstração:</u>

($\Longrightarrow$) Se $n > 1$ é *primo*, então cada um dos inteiros positivos *menores* que $\underline{n}$ é *primo* com $\underline{n}$ e, portanto,

$$\phi(n) = n - 1.$$

($\Longleftarrow$) Reciprocamente, se $\phi(n) = n - 1$, com $n > 1$, então $\underline{n}$ é *primo*, pois, se $\underline{n}$ fosse *composto*, teria pelo menos um divisor $\underline{d}$ tal que $1 < d < n$, de modo que pelo menos *dois* dos inteiros $1,2,3,\ldots,n$ não seriam *primos* com $\underline{n}$, $\underline{d}$ e $\underline{n}$, isto é, $\phi(n) \leqslant n-2$. Logo, $\underline{n}$ é *primo*.

Teorema 15.3 Se p e *primo* e se k é um inteiro positivo, então:

$$\phi(p^k) = p^k - p^{k-1} = p^k(1 - 1/p)$$

Demonstração:

Obviamente, o $mdc(n,p^k) = 1$ se e somente se p *não divide* n ($p \nmid n$), e como existem p^{k-1} inteiros entre 1 e p^k que são *divisíveis* por p os inteiros:

$$p,\ 2p,\ 3p,\ \ldots,\ (p^{k-1})p$$

segue-se que o conjunto $\{1,2,\ldots,p^k\}$ contém exatamente $p^k - p^{k-1}$ inteiros que são *primos* com p^k, de modo que, pela definição da função ϕ de EULER, temos:

$$\phi(p^k) = p^k - p^{k-1}$$

Assim, p.ex.:

$$\phi(16) = \phi(2^4) = 2^4 - 2^3 = 16 - 8 = 8$$

isto é, existem 8 inteiros *menores* que 16 e *primos* com 16, que são os inteiros 1,3,5,7,9,11,13 e 15.

Teorema 15.4 Se $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ é a *decomposição canônica* do inteiro positivo $n > 1$, então:

$$\phi(n) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1})\ldots(p_r^{k_r} - p_r^{k_r-1}) =$$

$$= n(1 - 1/p_1)(1 - 1/p_2)\ldots(1 - 1/p_r)$$

ou seja:

$$\phi(n) = \prod_{i=1}^{r} (p_i^{k_i} - p_i^{k_i-1}) = n \prod_{i=1}^{r} (1 - 1/p_i)$$

<u>Demonstração:</u>

Usaremos o *"Teorema da indução matemática"* sobre <u>r</u>, número de fatores primos distintos de <u>n</u>.

A proposição é verdadeira para r = 1 (Teorema 15.3). Suponhamos, então, a proposição verdadeira para r = i. Como o

$$\text{mdc}(p_1^{k_1} p_2^{k_2} \ldots p_i^{k_i}, p_{i+1}^{k_i+1})$$

e $\phi(n)$ é uma *função aritmética multiplicativa* (Teorema 15.1), temos:

$$\phi\left[(p_1^{k_1} p_2^{k_2} \ldots p_i^{k_i}) p_{i+1}^{k_i+1}\right] = \phi(p_1^{k_1} p_2^{k_2} \ldots p_i^{k_i})\, \phi(p_{i+1}^{k_i+1})$$

ou seja

$$\phi\left[(p_1^{k_1} p_2^{k_2} \ldots p_i^{k_i}) p_{i+1}^{k_i+1}\right] = \phi(p_1^{k_1} p_2^{k_2} \ldots p_i^{k_i})(p_{i+1}^{k_i+1} - p_{i+1}^{k_{i+1}-1})$$

ou, à vista da *hipótese de indução:*

$$\phi(p_1^{k_1} p_2^{k_2} \cdots p_i^{k_i} p_{i+1}^{k_i+1}) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \cdots$$

$$(p_i^{k_i} - p_i^{k_i-1})(p_{i+1}^{k_i+1} - p_{i+1}^{k_{i+1}-1})$$

e isto significa que a proposição é verdadeira para r=i+1. Logo, a proposição é verdadeira para todo inteiro positivo r.

Exemplo 15.4 Calcular $\phi(7865)$.

Por ser $7865 = 5.11^2.13$, temos:

$$\phi(7865) = (5 - 1)(11^2 - 11)(13 - 1) = 4.110.12 = 5280$$

Exemplo 15.5 Calcular $\phi(1350)$.

Por ser $1350 = 2.3^3.5^2$, temos:

$$\phi(1350) = 1350(1 - 1/2)(1 - 1/3)(1 - 1/5) =$$

$$= 1350.1/2.2/3.4/5 = 360$$

15.3 PROPRIEDADES DA FUNÇÃO DE EULER

Teorema 15.5 Para todo inteiro positivo $n > 2$, $\phi(n)$ é um inteiro *par*.

Demonstração:

Se n é uma potência de 2, isto é, $n = 2^k$, com $k \geq 2$, então, pelo teorema 15.3:

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

que é um inteiro *par*.

Se, ao invés, n não é uma potência de 2, então n é divisível por um *primo ímpar* p, isto é:

$$n = p^k m, \quad \text{onde} \quad k \geq 1 \quad \text{e o} \quad mdc(p^k, m) = 1$$

E como $\phi(n)$ é uma *função aritmética multiplicativa* (Teorema 15.1), temos:

$$\phi(n) = \phi(p^k)\ \phi(m) = p^{k-1}(p - 1)\ \phi(m)$$

que é também um inteiro *par*, porque $2 | (p - 1)$.

Assim, $\phi(n)$ é um inteiro ímpar somente para n=1 e n=2:

$$\phi(1) = \phi(2) = 1$$

Teorema 15.6 Se p é um *primo*, então:

$$\sum_{i=0}^{k} \phi(p^i) = p^k$$

Demonstração:

Pelo teorema 15.3, temos:

$$\phi(p) = p - 1$$

$$\phi(p^2) = p^2 - p = p(p - 1)$$

$$\phi(p^3) = p^3 - p^2 = p^2(p - 1)$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p - 1)$$

Somando ordenadamente todas essas igualdades, obtemos:

$$\sum_{i=1}^{k} \phi(p^i) = (p - 1)(1 + p + p^2 + \ldots + p^{k-1})$$

ou seja:

$$\sum_{i=1}^{k} \phi(p^i) = (p - 1)\frac{p^k - 1}{p - 1} = p^k - 1$$

Portanto:

$$\sum_{i=0}^{k} \phi(p^i) = \phi(1) + p^k - 1 = 1 + p^k - 1 = p^k$$

Teorema 15.8 Para todo inteiro positivo $n > 1$, a *soma* dos inteiros positivos *menores* que n e que são *primos* com n é igual a

$$\frac{1}{2}\, n \,.\, \phi(n)$$

Demonstração:

Sejam

$$a_1,\ a_2,\ \ldots,\ a_{\phi(n)}$$

os inteiros positivos *menores* que n e que são *primos* com n. Como o $mdc(a,n) = 1$ se e somente se o $mdc(n-a,\ n)=1$, os inteiros positivos *menores* que n e que são *primos* com n podem ser expressos pelas diferenças:

$$n - a_1,\ n - a_2,\ \ldots,\ n - a_{\phi(n)}$$

Portanto:

$$a_1 + a_2 + \ldots + a_{\phi(n)} = (n-a_1) + (n-a_2) + \ldots + (n-a_{\phi(n)}) =$$

$$= n.\phi(n) - (a_1 + a_2 + \ldots + a_{\phi(n)})$$

o que implica:

$$a_1 + a_2 + \ldots + a_{\phi(n)} = \frac{1}{2}\, n.\phi(n)$$

Exemplo 15.8 Verificar o teorema 15.8 com $n = 15$.

Por ser $15 = 3.5$, temos:

$$\phi(15) = (3 - 1)(5 - 1) = 2.4 = 8$$

é igual a $\phi(n/d)$. E como cada um dos n inteiros 1,2,3,... ...,n pertence precisamente a uma *única classe* S_d, temos:

$$\sum_{d|n} \phi(n/d) = n$$

Mas, quando d *percorre* todos os divisores positivos de n, o mesmo ocorre com n/d e, portanto:

$$\sum_{d|n} \phi(n/d) = \sum_{d|n} \phi(n) = n$$

Exemplo 15.7 Verificar o teorema 15.7 (de GAUSS) com n=10.

Os divisores positivos de 10 são 1,2,5,10 e, portanto, as *classes* S_d são:

$$S_1 = \{ m \mid 1 \leq m \leq 10 \text{ e } mdc(m,10) = 1 \} = \{ 1,3,7,9 \}$$

$$S_2 = \{ m \mid 1 \leq m \leq 10 \text{ e } mdc(m,10) = 2 \} = \{ 2,4,6,8 \}$$

$$S_5 = \{ m \mid 1 \leq m \leq 10 \text{ e } mdc(m,10) = 5 \} = \{5\}$$

$$S_{10} = \{ m \mid 1 \leq m \leq 10 \text{ e } mdc(m,10) = 10\} = \{10\}$$

Estas *classes* contem $\phi(10) = 4$, $\phi(5) = 4$, $\phi(2) = 1$ e $\phi(1) = 1$ inteiros, respectivamente. Portanto:

$$\sum_{d|10} \phi(d) = \phi(10) + \phi(5) + \phi(2) + \phi(1) =$$
$$= 4 + 4 + 1 + 1 = 10$$

como devia ser.

Exemplo 15.6 Verificar o teorema 15.6 com $p = 2$ e $k = 3$.

Temos:

$$\phi(2^0) = \phi(1) = 1, \qquad \phi(2^1) = \phi(2) = 1$$

$$\phi(2^2) = 2^2 - 2 = 2, \quad \phi(2^3) = 2^3 - 2^2 = 4$$

Portanto:

$$\sum_{i=0}^{3} \phi(2^i) = \phi(2^0) + \phi(2^1) + \phi(2^2) + \phi(2^3) =$$

$$= 1 + 1 + 2 + 4 = 8 = 2^3$$

Teorema 15.7 (de GAUSS) Para todo inteiro positivo $n \geq 1$:

$$\sum_{d|n} \phi(d) = n$$

Demonstração:

Os inteiros $1,2,3,\ldots,n$ podem ser separados em *classes* mediante o seguinte critério: se d é um divisor positivo de n, então o inteiro m $(1 \leq m \leq n)$ é *incluido* na classe S_d desde que o $mdc(m,n) = d$, isto é, simbolicamente:

$$S_d = \{ m \mid 1 \leq m \leq n \quad e \quad mdc(m,n) = d \}$$

Como o $mdc(m,n) = d$ se e somente se o $mdc(m/d, n/d) = 1$, segue-se que o número de inteiros da *classe* S_d é igual ao número de inteiros positivos que não superam n/d e que são primos com n/d, isto é, o número de inteiros da *classe* S_d

isto é, há 8 inteiros positivos *menores* que 15 e que são *primos* com 15-são os inteiros: 1,2,4,7,8,11,13 e 14. Portanto:

$$1 + 2 + 4 + 7 + 8 + 11 + 13 + 14 = 60 =$$

$$= \frac{15}{2} \cdot 8 = \frac{15}{2} \cdot \phi(15)$$

15.4 TEOREMA DE EULER

<u>Lema</u>.-Sejam $\underline{a}$ e $n > 1$ inteiros tais que o $mdc(a,n) = 1$. Se

$$a_1, a_2, \ldots, a_{\phi(n)}$$

são os inteiros positivos *menores* que $\underline{n}$ e que são *primos* com $\underline{n}$, então cada um dos inteiros:

$$aa_1, aa_2, \ldots, aa_{\phi(n)}$$

é *congruente módulo* $\underline{n}$ a um dos inteiros

$$a_1, a_2, \ldots, a_{\phi(n)}$$

(não necessariamente nesta ordem).

<u>Demonstração:</u>

Dois quaisquer dos inteiros $aa_1, aa_2, \ldots, aa_{\phi(n)}$ são *incongruentes módulo* $\underline{n}$, pois, se fosse:

$$aa_i \equiv aa_j \pmod{n}, \quad \text{com} \quad 1 \leqslant i < j \leqslant \phi(n)$$

cancelando o fator comum $\underline{a}$ (Corolário 9.1), teríamos:

$$a_i \equiv a_j \pmod{n}$$

o que é uma *contradição*.

Por outro lado, como o

$$mdc(a_i,n) = 1 \ (i = 1,2,\ldots, \phi(n)) \text{ e o } mdc(a,n) = 1$$

segue-se que o $mdc(aa_i, n) = 1$. Assim sendo, para cada aa_i existe um *único* inteiro b_i, com $0 \leqslant b_i < n$, tal que $aa_i \equiv b_i \pmod{n}$. Além disso, por ser

$$mdc(b_i,n) = mdc(aa_i,n) = 1$$

então b_i é um dos inteiros $a_1,a_2,\ldots,a_{\phi(n)}$, isto é, os inteiros:

$$aa_1, aa_2, \ldots, aa_{\phi(n)} \quad \text{e} \quad a_1, a_2,\ldots, a_{\phi(n)}$$

são *idênticos* (módulo n) numa certa ordem, e a proposição fica demonstrada.

Teorema 15.9 (de EULER) Se n é um inteiro positivo e se o $mdc(a,n) = 1$, então:

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Demonstração:

Para $n = 1$ a proposição é verdadeira, pois, temos:

$$a^{\phi(1)} = a \equiv 1 \pmod{.1}$$

Suponhamos, pois, $n > 1$. Sejam $a_1, a_2, \ldots, a_{\phi(n)}$ os inteiros positivos *menores* que $\underline{n}$ e que são *primos* com $\underline{n}$. Como o $mdc(a,n) = 1$, então, pelo *lema* anterior, os inteiros

$$aa_1,\ aa_2,\ \ldots,\ a_{\phi(n)}$$

são *congruentes módulo* $\underline{n}$, não necessariamente nesta ordem, aos inteiros $a_1, a_2, \ldots, a_{\phi(n)}$, isto é:

$$\begin{aligned} aa_1 &\equiv a_1^* \pmod{.n} \\ aa_2 &\equiv a_2^* \pmod{.n} \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ aa_{\phi(n)} &\equiv a_{\phi(n)}^* \pmod{.n} \end{aligned}$$

onde $a_1^*, a_2^*, \ldots, a_{\phi(n)}^*$ são os inteiros

$$a_1, a_2, \ldots, a_{\phi(n)}$$

numa certa ordem.

Multiplicando ordenadamente essas $\phi(n)$ congruências, obtemos:

$$\begin{aligned} (aa_1)(aa_2)\ \ldots\ (aa_{\phi(n)}) &\equiv a_1^* a_2^* \ldots a_{\phi(n)}^* \pmod{.n} \\ &\equiv a_1 a_2 \ldots a_{\phi(n)} \pmod{.n} \end{aligned}$$

ou seja:

$$a^{\phi(n)}\ (a_1a_2\ldots a_{\phi(n)}) \equiv a_1a_2\ldots a_{\phi(n)} (\text{mod}.n)$$

Como o $\text{mdc}(a_i,n) = 1$ para $i = 1,2,3,\ldots, \phi(n)$, então o

$$\text{mdc}(a_1a_2\ldots a_{\phi(n)},\ n) = 1$$

e, portanto, podemos *cancelar* o fator comum

$$a_1a_2\ \ldots\ a_{\phi(n)},$$

o que dá:

$$a^{\phi(n)} \equiv 1\ (\text{mod}.n)$$

Note-se que, se <u>p</u> é um *primo*, então $\phi(p) = p-1$, e se o $\text{mdc}(a,p) = 1$:

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

que é o *teorema de FERMAT*. Assim, o *teorema de EULER* é uma *generalização* do *teorema de FERMAT*.

<u>Exemplo 15.9</u> Verificar o *teorema de EULER* com $n = 9$ e $a = -4$.

O $\text{mdc}(-4,9) = 1$ e $\phi(9) = 6$. Portanto:

$$(-4)^{\phi(9)} = (-4)^6 = 4096$$

E como $9|(4096 - 1)$, segue-se que

$$4096 \equiv 1 \pmod{9}, \quad \text{isto é:} \quad (-4)^{\phi(9)} \equiv 1 \pmod{9}$$

<u>Exemplo 15.10</u> Usando o *teorema de EULER*, resolver a congruência linear $ax \equiv b \pmod{m}$, onde o $mdc(a,m) = 1$.

Pelo *teorema de EULER*, temos:

$$a^{\phi(m)} \equiv 1 \pmod{m}, \quad \text{ou:} \quad a^{\phi(m)} b \equiv b \pmod{m}$$

Portanto:

$$ax \equiv a^{\phi(m)} b \pmod{m}$$

Como o $mdc(a,m) = 1$, podemos *cancelar* o fator comum <u>a</u>, o que dá:

$$x \equiv a^{\phi(m)-1} b \pmod{m}$$

Consideremos, p.ex., a congruência linear $3x \equiv 5 \pmod{8}$, onde o $mdc(3,8) = 1$. Temos:

$$x \equiv 3^{\phi(8)-1}.5 \equiv 3^{4-1}.5 \equiv 135 \pmod{8}$$

15.5 RELAÇÃO ENTRE AS FUNÇÕES ϕ E u

<u>Teorema 15.8</u> Para todo inteiro $n \geq 1$:

$$\phi(n) = n \sum_{d|n} u(d)/d$$

Demonstração:

Pelo teorema 15.7 (de GAUSS), temos:

$$n = \sum_{d|n} \phi(d)$$

e, portanto, pela *fórmula de inversão de* MOBIUS:

$$\phi(n) = \sum_{d|n} u(d)(n/d) = n \sum_{d|n} u(d)/d$$

fórmula importante que relaciona as funções ϕ de EULER e u de MOBIUS.

Assim, p.ex.:

$$\phi(8) = 8 \sum_{d|8} u(d)/d = 8(u(1)/1 + u(2)/2 + u(4)/4+u(8)/8)=$$

$$= 8(1/1 + (-1)/2 + 0/4 + 0/8) = 8(1 - 1/2) = 4$$

EXERCÍCIOS

1. Calcular: $\phi(420)$, $\phi(1001)$, $\phi(5040)$ e $\phi(8316)$.

2. Calcular: $d(\phi(15))$ e $\phi(d(15))$.

3. Calcular: $(\phi(p)s(p) + 1)/p$, sendo p um *primo*.

4. Verificar que $\phi(n+2) = \phi(n) + 2$ para $n = 12,14,20$.

5. Verificar que $\phi(n) = \phi(n+1) = \phi(n+2)$ para $n = 5186$.

6. Verificar que $\phi(3^k.568) = \phi(3^k.638)$, onde o inteiro $k \geq 0$.

7. Verificar que $\phi(n)$ é uma *função aritmética multiplicativa* para $n = 144$.

8. Mostrar que $\phi(n)$ não é uma *função aritmética multiplicativa completa*.

9. Verificar o *teorema de EULER* com $n = 10$ e $a = 3$.

10. Usando o teorema de EULER, resolver as seguintes congruências lineares:

(a) $5x \equiv 7 \pmod{12}$ (b) $2x \equiv 3 \pmod{9}$

(c) $7x \equiv 1 \pmod{10}$ (d) $8x \equiv 4 \pmod{5}$

(e) $2x \equiv 1 \pmod{17}$ (f) $5x \equiv -3 \pmod{8}$

11. Demonstrar que $\phi(n^2) = n.\phi(n)$ para todo inteiro positivo $\underline{n}$.

12. Demonstrar que, se $\underline{n}$ é um inteiro positivo *ímpar*, então:

(a) $\phi(2n) = \phi(n)$ (b) $\phi(4n) = 2\phi(n)$

13. Mostrar que o $mdc(m,n) = 2$ implica

$$\phi(mn) = 2\phi(m)\phi(n).$$

14. Demonstrar que o número de frações positivas irredutíveis menores ou iguais a 1 com denominador $\underline{n}$ é igual a $\phi(n)$.

15. Verificar o teorema 15.6 com $p = 3$ e $k = 4$.

16. Verificar o teorema 15.8 com $n = 17$ e $n = 28$.

17. Verificar o teorema 15.7 (de GAUSS) com $n = 36,105,147$.

18. Mostrar que, se $\underline{n}$ é um inteiro *par*, então:

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

19. Demonstrar que $\phi(3n) = 3\phi(n)$ se e somente se $3|n$.

20. Demonstrar que $\phi(n) = \frac{n}{2}$ se e somente se $n = 2^k$, onde $k \geqslant 1$.

21. Demonstrar que $\sqrt{n}/2 \leqslant \phi(n) \leqslant n$ para todo inteiro positivo $\underline{n}$.

22. Demonstrar que, se o inteiro $n > 1$ tem $\underline{r}$ fatores *primos* distintos, então

$$\phi(n) \geqslant n/2^r.$$

23. Demonstrar que, se o inteiro $n > 1$ é *composto*, então

$$\phi(n) \leqslant n - \sqrt{n}.$$

24. Demonstrar que, se o inteiro positivo $\underline{n}$ tem $\underline{r}$ fatores *primos ímpares* distintos, então

$$2^r \mid \phi(n).$$

25. Demonstrar que, se $\underline{n}$ e $n+2$ são *primos gêmeos*, então:

$$\phi(n + 2) = \phi(n) + 2$$

26. Demonstrar que, se $n = 2^k$ ou $n = 2^k 3^j$, onde $\underline{k}$ e $\underline{j}$ são inteiros positivos, então $\phi(n) \mid n$.

27. Demonstrar que, se $d \mid n$, então

$$\phi(d) \mid \phi(n).$$

CAPÍTULO 16

NÚMEROS PERFEITOS

16.1 NÚMEROS PERFEITOS

Definição 16.1 Um inteiro positivo n diz-se um *número perfeito* se e somente se é igual à soma de todos os seus divisores positivos, *exceto* o divisor trivial n.

A soma de todos os divisores positivos de n, com *exceção* do divisor n, é igual a $s(n) - n$ e, portanto, n é um *número perfeito* se e somente se a seguinte condição se verifica:

$$n = s(n) - n, \quad \text{ou:} \quad s(n) = 2n$$

isto é, um inteiro positivo n é um *número perfeito* se e somente se a soma de todos os seus divisores positivos é igual ao seu *dobro* 2n.

Assim, p.ex., para $n = 6$ e $n = 28$, temos:

$$s(6) = 1 + 2 + 3 + 6 = 12 = 2.6$$

$$s(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56 = 2.28$$

de modo que os inteiros positivos 6 e 28 são ambos *números perfeitos*.

Os números perfeitos são muito *raros* e até hoje (1980) são conhecidos apenas 24, todos *pares*, e os seis primeiros são:

$$P_1 = 6, \quad P_2 = 28, \quad P_3 = 496$$

$$P_4 = 8128, \quad P_5 = 33550336, \quad P_6 = 8589869056$$

os quais *terminam* em 6 ou em 8 e, com exceção de 6, são da *forma* 9k+1.

Não se conhece nenhum número perfeito *ímpar*, e nem mesmo se sabe se existem, mas, se existem, são muito grandes - maiores que 10^{50}.

<u>Teorema 16.1</u> (de EUCLIDES) Se $2^k - 1$ é *primo* $(k > 1)$, então o inteiro positivo $n = 2^{k-1}(2^k-1)$ é um *número perfeito*.

<u>Demonstração:</u>

Seja $2^k-1 = p(k > 1)$ um *primo*. Consideremos o inteiro positivo $n = 2^{k-1}p$. Como o $mdc(2^{k-1},p) = 1$ e $s(n)$ é uma *função aritmética multiplicativa*, temos:

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

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

Logo, por definição, n é um *número perfeito*.

Assim, todas as vezes que se conhece um inteiro $k > 1$ tal que $2^k - 1$ é *primo* pode-se construir um *número perfeito*. Para $k = 13$, p.ex., temos $2^{13} - 1 = 8191$, um *primo*, o que dá o 5 *número perfeito:*

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

NOTA. Os quatro primeiros *números perfeitos* se obtem pela fórmula de EUCLIDES atribuindo a k os valores 2,3,5 e 7, isto é:

$$P_1 = 2(2^2 - 1) = 6, \qquad P_2 = 2^2(2^3 - 1) = 28$$

$$P_3 = 2^4(2^5 - 1) = 496, \qquad P_4 = 2^6(2^7 - 1) = 8128$$

Para $k = 17$ e $k = 19$, a fórmula de EUCLIDES dá-nos o *sexto* e o *sétimo números perfeitos:*

$$P_6 = 2^{16}(2^{17} - 1) \quad \text{e} \quad P_7 = 2^{18}(2^{19} - 1)$$

os quais foram determinados, pela primeira vez, pelo matemático italiano PIETRO CATALDI em 1603.

Os outros 17 *números perfeitos* conhecidos se obtem pela

fórmula de EUCLIDES atribuindo a k os seguintes valores:

31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213 e 19937

Teorema 16.2 (de EULER) Se n é um *número perfeito par*, então:

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

onde $2^k - 1$ é *primo*.

Demonstração:

Suponhamos que n é um *número perfeito par*. Então, n pode escrever-se sob a forma: $n = 2^{k-1}m$, onde m é um inteiro *ímpar* e $k \geqslant 2$.

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

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

Por outro lado, como n é um *número perfeito*, temos:

$$s(n) = 2n = 2^k m$$

Portanto:

$$2^k m = (2^k - 1)s(m) \qquad (1)$$

de modo que $(2^k - 1) | 2^k m$. Mas, o $mdc(2^k - 1, 2^k) = 1$, o que implica:

$$(2^k - 1) | m, \quad \text{isto é:} \quad m = (2^k - 1)M$$

Substituindo este valor de $\underline{m}$ em (1) e *cancelando* o fator comum $2^k - 1$, obtemos:

$$s(m) = 2^k M$$

Como $\underline{m}$ e $\underline{M}$ são ambos divisores positivos de $\underline{m}$ (com $M < m$), temos:

$$2^k M = s(m) \geqslant m + M = 2^k M$$

o que implica:

$$s(m) = m + M$$

Assim sendo, $\underline{m}$ e $\underline{M}$ são os únicos divisores positivos de $\underline{m}$, e isto significa que $\underline{m}$ é *primo* e $M = 1$. Então:

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

é um *primo*, e por ser

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

o *teorema de EULER* fica demonstrado.

Este teorema é o *recíproco* do teorema 16.1 (de EUCLIDES) e foi demonstrado por EULER cerca de 2000 anos depois de EUCLIDES.

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

$$2^k - 1 \ (k \geqslant 2)$$

seja *primo*.

<u>Teorema 16.3</u> Se $2^k - 1 \ (k \geqslant 2)$ é *primo*, então <u>k</u> também é *primo*.

<u>Demonstração:</u>

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

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

ou seja:

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

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

NOTA. O *recíproco* deste teorema 16.3 é *falso*, isto é, <u>k</u> *primo* não implica $2^k - 1$ também *primo*. Assim, p.ex., 11 é *primo* e no entanto $2^{11} - 1$ é *composto*, pois, temos:

$$2^{11} - 1 = 2047 = 23.89$$

Teorema 16.4 **Todo número perfeito par termina em 6 ou 8.**

Demonstração:

Seja n um número perfeito par. Pelo teorema 16.2 (de EULER), temos:

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

E, pelo teorema 16.3, sendo $2^k - 1$ *primo*, k também é *primo*. Se $k = 2$, então $n = 6$, e a proposição é verdadeira. Suponhamos, pois, $k > 2$. Todo *primo maior que* 2 é da forma $4m+1$ ou $4m+3$. Se k é da forma $4m+1$, então:

$$n = 2^{4m}\,(2^{4m+1} - 1) = 2^{8m+1} - 2^{4m} = 2.16^{2m} - 16^m$$

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

$$n \equiv 2.6 - 6 \equiv 6 \pmod{10}, \text{ isto é: } n = 10h + 6$$

e, portanto, n *termina em* 6.

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

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

$$= 2.16^{2m+1} - 4,16^m$$

Por ser $16^t \equiv 6 \pmod{10}$, qualquer que seja o inteiro posi

tivo t, segue-se que

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

isto é:

$$n = 10h^{*} + 8$$

e, portanto, n *termina em* 8.

Corolário 16.1 Todo número perfeito par n é *congruente a* 6 *módulo* 10 ou *congruente a* 8 *módulo* 10, isto é:

$$n \equiv 6 \pmod{10} \quad \text{ou} \quad n \equiv 8 \pmod{10}$$

Teorema 16.5 Um *primo* não pode ser um *número perfeito*.

Demonstração:

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

$$p + 1 = 2p \quad \text{e} \quad p = 1$$

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

16.2 NÚMEROS MULTIPERFEITOS

Definição 16.2 Um inteiro positivo n diz-se que um *número*

multiperfeito de ordem k ou um k-*número perfeito* se e somente se $s(n) = kn$, onde $k \geqslant 3$ é um inteiro.

Assim, p.ex., o inteiro positivo $30240 = 2^5.3^3.5.7$ é um *número multiperfeito de ordem* 4, pois, temos:

$$s(30240) = \frac{2^6 - 1}{2 - 1} \cdot \frac{3^4 - 1}{3 - 1} \cdot \frac{5^2 - 1}{5 - 1} \cdot \frac{7^2 - 1}{7 - 1} =$$

$$= 63.40.6.8 = 120960 = 4.30240$$

16.3 NÚMEROS AMIGOS

Definição 16.3 Dois inteiros positivos m e n dizem-se *números amigos* se e somente se a soma dos divisores positivos de m, *exceto* o divisor m, é igual a n, e a soma dos divisores positivos de n, *exceto* o divisor n, é igual a m.

Em outros termos, dois inteiros positivos m e n dizem-se *números amigos* se e somente se

$$s(m) - m = n \quad e \quad s(n) - n = m$$

ou seja, o que é equivalente:

$$s(m) = m + n = s(n)$$

Exemplo 16.1 Mostrar que os inteiros 220 e 284 são *números amigos.*

Por ser

$$220 = 2^2.5.11 \quad e \quad 284 = 2^2.71$$

temos:

$$s(220) - 220 = s(2^2)s(5)s(11) - 220 =$$

$$= 7.6.12 - 220 = 504 - 220 = 284;$$

$$s(284) - 284 = s(2^2)s(71) - 284 =$$

$$= 7.72 - 284 = 504 - 284 = 220$$

isto é:

$$s(220) = 220 + 284 = s(284)$$

Logo, por definição, os inteiros 220 e 284 são *números amigos.*

16.4 NÚMEROS DEFICIENTES E ABUNDANTES

Definição 16.4 Um inteiro positivo n diz-se um *número deficiente* se e somente se

$$s(n) - n < n \quad ou \quad s(n) < 2n$$

e diz-se um *número abundante* se e somente se

$$s(n) - n > n \quad \text{ou} \quad s(n) > 2n$$

Assim, p.ex., os inteiros 15 e 18 são respectivamente um *número deficiente* e um *número abundante*, pois, temos:

$$s(15) = s(3.5) = s(3)s(5) = 4.6 = 24 < 2.15$$

$$s(18) = s(2.3^2) = s(2)s(3^2) = 3.13 = 39 > 2.18$$

16.5 NÚMEROS DE MERSENNE

<u>Definição 16.5</u> Chama-se *número de MERSENNE* todo inteiro positivo da forma:

$$M_n = 2^n - 1 \quad (n \geqslant 2)$$

Se M_n é *primo* diz-se que é um *primo de MERSENNE*.

A tradicional denominação de "números de MERSENNE" dada aos *inteiros* M_n é uma homenagem ao matemático do século XVII MARIN MERSENNE (1588-1648) que, interessado em encontrar *números perfeitos*, estudou os *inteiros* M_n. Como resultado das suas pesquisas MERSENNE fez em 1644 a seguinte *afirmação:* Todo inteiro $M_p = 2^p - 1$ é *primo* para

$$p = 2,3,5,7,13,17,19,31,67,127,257$$

e é *composto* para todos os outros *primos* $p < 257$.

Esta *afirmação*, entretanto, é *incorreta*, pois, sabe-se hoje que são *primos de MERSENNE* os 24 seguintes inteiros:

$$M_2, M_3, M_5, M_7, M_{13}, M_{17}, M_{19}, M_{31}, M_{61}, M_{89}, M_{107}, M_{127}, M_{521},$$

$$M_{607}, M_{1279}, M_{2203}, M_{2281}, M_{3217}, M_{4253}, M_{4423}, M_{9689},$$

$$M_{9941}, M_{11213}, M_{19937}$$

e que para todos os demais valores de $p \leqslant 257$ os inteiros M_p são *compostos*, exceto possivelmente para

$$p = 157,\ 167,\ 193,\ 199,\ 227,\ 229$$

porque, para estes 6 valores de p não se sabe ainda se M_p é *primo* ou se é *composto*.

Como se vê, MERSENNE cometeu dois *enganos: incluiu* M_{67} e M_{257} na sua *lista de primos* e *excluiu* dessa *lista* M_{61}, M_{89} e M_{107}.

É interessante notar que os quatro primeiros *primos de MERSENNE são:*

$$M_2 = 3,\quad M_5 = 7,\quad M_5 = 31,\quad M_7 = 127$$

e que

$$M_{M_2} = M_3,\quad M_{M_3} = M_7,\quad M_{M_5} = M_{31},\quad M_{M_7} = M_{127}$$

também são *primos de MERSENNE*. Entretanto, o quinto *primo de MERSENNE* é $M_{13} = 8191$, mas

$$M_{M_{13}} = M_{8191} = 2^{8191} - 1$$

não é um primo de MERSENNE, pois, é um inteiro *composto* com 2466 algarismos. Assim, é *falsa* a *conjectura*: Se M_n é um *primo de MERSENNE*, então M_{M_n} também é um *primo de MERSENNE*.

<u>Teorema 16.6</u> Se <u>p</u> e $q = 2p + 1$ são primos, então:

$$q | M_p \quad \text{ou} \quad q | M_p + 2$$

mas <u>q</u> não divide conjuntamente M_p e $M_p + 2$.

<u>Demonstração:</u>

Como <u>q</u> é *primo* e o $mdc(2,q) = 1$, temos, pelo teorema de FERMAT:

$$2^{q-1} - 1 \equiv 0 \ (\text{mod.}q)$$

ou, fatorando o 1º membro:

$$(2^{(q-1)/2} - 1)(2^{(q-1)/2} + 1) \equiv 0 \ (\text{mod.}q)$$

ou seja:

$$M_{(q-1)/2} \ (M_{(q-1)/2} + 2) \equiv 0 \ (\text{mod.}q)$$

ou, por ser $(q-1)/2 = p$:

$$M_p(M_p + 2) \equiv 0 \ (\text{mod.}q)$$

Assim, $\underline{q}$ é um *primo* que divide o produto $M_p(M_p + 2)$ e, portanto, $q|M_p$ ou $q|M_p + 2$ (Corolário 7.1). Mas, $\underline{q}$ não divide conjuntamente M_p e $M_p + 2$, porque, então, $q|2$, o que é impossível.

<u>Exemplo 16.2</u> Demonstrar que o número de MERSENNE M_{23} é *composto*.

Como os inteiros $p = 23$ e $q = 2.23 + 1 = 47$ são *primos*, segue-se que

$$47|M_{23} \quad \text{ou} \quad 47|M_{23} + 2$$

e cumpre demonstrar que se verifica a primeira alternativa. Com efeito, temos:

$$2^{23} = 2^3(2^5)^4 \equiv 2^3(-15)^4 \pmod{47}$$

e

$$(-15)^4 = (225)^2 \equiv (-10)^2 \equiv 6 \pmod{47}$$

Portanto:

$$2^{23} \equiv 2^3.6 \equiv 48 \equiv 1 \pmod{47}$$

isto é:

$$2^{23} - 1 = M_{23} \equiv 0 \pmod{47}$$

e isto significa que $47|M_{23}$, de modo que M_{23} é *composto*.

16.6 NÚMEROS DE FERMAT

Definição 16.6 Chama-se *número de FERMAT* todo inteiro positivo da forma:

$$F_n = 2^{2^n} + 1 \quad (n \geq 0)$$

Se F_n é *primo* diz-se que é um *primo de FERMAT*.

Observou FERMAT, em 1640, que os inteiros positivos:

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537$$

são todos *primos* e *conjecturou:* F_n é *primo* para todo inteiro $n \geq 0$.

Entretanto, EULER, em 1732, derrubou a *conjectura de FERMAT*, mostrando que F_5 é *composto* - precisando que $641 | F_5$, isto é:

$$F_5 = 2^{32} + 1 = 4294967297 = (641).(6700417)$$

Até hoje não se conseguiu encontrar um *primo de FERMAT* distinto dos cinco primeiros. Realmente, para $5 \leq n \leq 16$ cada *número de FERMAT* F_n é composto, e também é sabido que F_n é composto para os 34 seguintes valores isolados de n:

n = 18,19,21,23,25,26,27,30,32,36,38,39,42,52,55,
58,63,73,77,81,117,125,144,150,207,226,228,
260,267,268,284,316,452,1945.

Portanto, o melhor é "conjecturar" que todos os $F_n > F_4$ são inteiros *compostos*.

<u>Teorema 16.7</u> Se F_n e F_m são dois *números de FERMAT*, com $m > n \geq 0$, então o $mdc(F_n, F_m) = 1$.

<u>Demonstração:</u>

Seja $d = mdc(F_n, F_m)$. Como os números de FERMAT são inteiros *ímpares*, segue-se que <u>d</u> também é um inteiro *ímpar*. Temos:

$$\frac{F_m - 2}{F_n} = (2^{2^m} - 1)/(2^{2^n} + 1) =$$

$$= \left[(2^{2^n})^{2^{m-n}} - 1 \right] / (2^{2^n} + 1)$$

Denotando, para simplicidade de notação, 2^{2^n} por <u>x</u> e 2^{m-n} por <u>k</u>, temos:

$$\frac{F_m - 2}{F_m} = \frac{x^k - 1}{x + 1} = x^{k-1} - x^{k-2} + \ldots - 1$$

de modo que $F_n | (F_m - 2)$. Como $d | F_n$, segue-se que $d | (F_m - 2)$.

Mas, $d | F_m$ e, portanto, $d | 2$. E como <u>d</u> é um inteiro *ímpar*, temos $d = 1$.

EXERCÍCIOS

1. Mostrar que o inteiro 130816 não é um número perfeito.

2. Mostrar que o inteiro $n = 2^{10}(2^{11} - 1)$ não é um número perfeito.

3. Demonstrar as seguintes proposições:

   (a) Nenhuma potência de um *primo* é um *número perfeito*.

   (b) Um *quadrado perfeito* não pode ser um *número perfeito*.

   (c) O produto de dois *primos ímpares* nunca é um *número perfeito*.

4. Demonstrar que, se $\underline{n}$ é um *número perfeito*, então:

$$\sum_{d|n} 1/d = 2.$$

5. Demonstrar que todo *número perfeito par* é um *número triangular*.

6. Demonstrar que se $\underline{n}$ é um *número perfeito par:*

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

então:

(a) $n = 1 + 2 + 3 + \ldots + (2^k - 1)$

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

7. Mostrar que, se $n > 6$ é um *número perfeito par*, então a soma dos seus algarismos é *congruente a* 1 (mod.9).

8. Mostrar que nenhum *divisor* de um *número perfeito* pode ser um *número perfeito*.

9. Achar os dois últimos algarismos do *número perfeito:*

$$n = 2^{19936}\,(2^{19937} - 1)$$

10. Mostrar que, se $\underline{n}$ é um *número perfeito par*, então $8n+1$ é um *quadrado perfeito*.

11. Mostrar que os inteiros 120 e 672 são *números multiperfeitos*.

12. Mostrar que o inteiro:

    (a) 523776 é um 3-número perfeito;

    (b) 2178540 é um 4-número perfeito;

    (c) 14182439040 é um 5-número perfeito.

13. Demonstrar as seguintes proposições:

    (a) Se $\underline{n}$ é um 3-número perfeito e se $3 \nmid n$, então $\underline{3n}$ é um 4-número perfeito.

    (b) Se $\underline{n}$ é um 5-número perfeito e se $5 \nmid n$, então $\underline{5n}$ é um 6-número perfeito.

    (c) Se $\underline{3n}$ é um 4k-número perfeito e se $3 \nmid n$, então $\underline{n}$ é um 3k-número perfeito.

14. Mostrar que 120 e 672 são os *únicos* 3-números perfeitos da forma $n = 2^k.3.p$, onde $\underline{p}$ é um *primo ímpar*.

15. Demonstrar que, se $n > 6$ é um número perfeito par, então $\underline{n}$ é *congruente a* 1 (módulo 6).

16. Mostrar que são *números amigos* os inteiros:

    (a) 2620 e 2924 (b) 17296 e 18416

17. Classificar os inteiros 2,3,4,...,21 como números *deficientes, perfeitos* ou *abundantes*.

18. Mostrar que o inteiro $945 = 3^3.5.7$ é um *número abundante* e determinar um outro *número abundante* da forma $3^k.5.7$.

19. Demonstrar que todo *múltiplo* de um número perfeito é um *número abundante*.

20. Mostrar que, se $n > 3$ e se $2n+1$ é *primo*, então $2n(2n+1)$ é um *número deficiente*.

21. Mostrar que, se $\underline{n}$ é um número perfeito par e se $\underline{d}$ *divide* $\underline{n}$ $(d|n)$, onde $1 < d < n$, então $\underline{d}$ é um *número deficiente*.

22. Mostrar que nenhum inteiro da forma $n = 2^a.3^b$ é um 3-número perfeito.

23. Seja m, n um par de *números amigos*. Demonstrar:

(a) Se $m > n$, então m é um *número deficiente*.

(b) Se m é *par* e se n é ímpar, então n é um *quadrado perfeito*.

24. Determinar o *primo de MERSENNE* M_{19}.

25. Mostrar que os *números de MERSENNE* M_{11} e M_{29} são inteiros *compostos*.

26. Um inteiro positivo n diz-se um *número superperfeito* se e somente se $s(s(n)) = 2n$. Mostrar que, se $n = 2^k$ e se $2^{k+1} - 1$ é *primo*, então n é um *número superperfeito*.

27. Mostrar que 5 e 7 são os *únicos primos gêmeos* cuja semi-soma é um *número perfeito*.

28. Seja $n = 2^{k-1}(2^k - 1)$ um número perfeito par. Demonstrar que o produto dos divisores positivos de n é igual a n^k.

CAPÍTULO 17

NÚMEROS DE FIBONACCI

17.1 SEQUÊNCIAS RECORRENTES

Consideremos a *sequência* de inteiros:

$$u_1, u_2, u_3, \ldots, u_{n-1}, u_n, \ldots \qquad (1)$$

na qual cada termo, a partir do *terceiro*, é a soma dos dois termos precedentes, isto é, para todo $n \geqslant 3$:

$$u_n = u_{n-1} + u_{n-2} \qquad (2)$$

Tais sequências, nas quais a partir de um determinado termo, cada um dos seguintes é uma *combinação linear* de termos anteriores, ocorrem com frequência em Matemática e recebem o nome de *sequências recorrentes*. O processo pelo qual se determinam sucessivamente os termos particulares destas sequências chama-se *processo recorrente* e uma igualdade da forma (2) é uma *fórmula recorrente*.

É óbvio que se podem construir arbitrariamente um número infinito de sequências de inteiros satisfazendo à condição (2), tais como, p.ex.:

$$2,5,7,12,19,31,50, \ldots$$
$$1,3,4,7,11,18,29, \ldots$$
$$-1,-5,-6,-11,-17, \ldots$$

Como se vê, a condição (2) não basta para determinar univocamente a sequência (1), sendo necessário conhecer os seus *dois primeiros termos* para poder calcular todos os outros, isto é, conhecer ou fixar os termos u_1 e u_2.

17.2 SEQUÊNCIA DE FIBONACCI

A sequência de inteiros:

$$F_1, F_2, F_3, \ldots, F_{n-1}, F_n, \ldots$$

no caso em que

$$F_1 = F_2 = 1 \quad e \quad F_n = F_{n-1} + F_{n-2} \ (n \geq 3)$$

isto é, a sequência:

$$1,1,2,3,5,8,13,21,34,55,89,144,233,377,\ldots$$

recebe o nome de *sequência de FIBONACCI* e os seus termos chamam-se *números de FIBONACCI*.

Os *números de FIBONACCI* (ou LEONARDO DE PISA, famoso matemático italiano do século XIII (1180-1250) possuem muitas propriedades importantes e aqui vamos estudar algumas delas.

17.3 SOMAS DE NÚMEROS DE FIBONACCI

Teorema 17.1 A soma dos n primeiros *números de FIBONACCI* é igual a $F_{n+2} - 1$.

Demonstração:

Com efeito, temos:

$$F_1 = F_3 - F_2$$
$$F_2 = F_4 - F_3$$
$$F_3 = F_5 - F_4$$
$$\cdots\cdots\cdots\cdots$$
$$F_{n-1} = F_{n+1} - F_n$$
$$F_n = F_{n+2} - F_{n+1}$$

Somando ordenadamente todas essas n igualdades e simplificando, obtemos:

$$F_1 + F_2 + F_3 + \ldots + F_{n-1} + F_n = F_{n+2} - F_2 = F_{n+2} - 1$$

Assim, p.ex.:

$$1 + 1 + 2 + 3 + 5 + 8 + 13 + 21 = F_{10} - 1 = 55 - 1 = 54$$

Teorema 17.2 A soma dos n primeiros *números de FIBONACCI* com *índices ímpares* é igual a F_{2n}.

Demonstração:

Com efeito, temos:

$$F_1 = F_2$$
$$F_3 = F_4 - F_2$$
$$F_5 = F_6 - F_4$$
$$\cdots\cdots\cdots\cdots$$
$$F_{2n-3} = F_{2n-2} - F_{2n-4}$$
$$F_{2n-1} = F_{2n} - F_{2n-2}$$

Somando ordenadamente todas essas n igualdades e simplificando, obtemos:

$$F_1 + F_3 + F_5 + \ldots + F_{2n-3} + F_{2n-1} = F_{2n}$$

Assim, p.ex.:

$$1 + 2 + 5 + 13 + 34 + 89 + 233 = F_{14} = 377$$

Teorema 17.3 A soma dos n primeiros *números de FIBONACCI* com *índices pares* é igual a $F_{2n+1} - 1$.

Demonstração:

Com efeito, temos:

$$F_2 = F_3 - F_1$$
$$F_4 = F_5 - F_3$$
$$F_6 = F_7 - F_5$$
$$\cdots\cdots\cdots\cdots$$
$$F_{2n-2} = F_{2n-1} - F_{2n-3}$$
$$F_{2n} = F_{2n+1} - F_{2n-1}$$

Somando ordenadamente todas essas n igualdades e simplificando, obtemos:

$$F_2 + F_4 + F_6 + \ldots + F_{2n-2} + F_{2n} = F_{2n+1} - F_1 = F_{2n+1} - 1$$

Assim, p.ex.:

$$1 + 3 + 8 + 21 + 55 + 144 = F_{13} - 1 = 233 - 1 = 232$$

Teorema 17.4 A soma dos n primeiros *números de FIBONACCI* tomados alternadamente com os sinais + e - é igual a $(-1)^{n+1}F_{n-1} + 1$.

Demonstração:

Com efeito, subtraindo ordenadamente as igualdades correspondentes aos teoremas 17.2 e 17.3, temos:

$$F_1 - F_2 + F_3 - F_4 + \ldots + F_{2n-1} - F_{2n} = F_{2n} - F_{2n+1} + 1 =$$

$$= -F_{2n+1} + 1 \qquad (3)$$

Somando F_{2n+1} a ambos os membros desta igualdade, temos:

$$F_1 - F_2 + F_3 - F_4 + \ldots + F_{2n-1} - F_{2n} - F_{2n+1} = -F_{2n-1} + 1 +$$

$$+ F_{2n+1} = F_{2n} + 1 \qquad (4)$$

Consoante as igualdades (3) e (4), temos:

$$F_1 - F_2 + F_3 - F_4 + \ldots + (-1)^{n+1} F_n = (-1)^{n+1} F_{n-1} + 1$$

Assim, p.ex.:

$$1 - 1 + 2 - 3 + 5 - 8 + 13 - 21 =$$

$$= (-1)^9 F_7 + 1 = -13 + 1 = 12;$$

$$1 - 1 + 2 - 3 + 5 - 8 + 13 - 21 + 34 =$$

$$= (-1)^{10} F_8 + 1 = 21 + 1 = 22$$

17.4 SOMA DOS QUADRADOS DE NÚMEROS DE FIBONACCI

Teorema 17.5 A soma dos quadrados dos n primeiros *números de FIBONACCI* é igual a $F_n F_{n+1}$.

Demonstração:

Por ser $F_1 = F_2 = 1$, temos $(F_1)^2 = F_1 F_2$, e para $k > 1$, temos:

$$F_k F_{k+1} - F_{k-1} F_k = F_k (F_{k+1} - F_{k-1}) = (F_k)^2$$

Fazendo nesta igualdade $k = 2,3,\ldots,n$, temos:

$$(F_1)^2 = F_1 F_2$$

$$(F_2)^2 = F_2 F_3 - F_1 F_2$$

$$(F_3)^2 = F_3 F_4 - F_2 F_3$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$(F_{n-1})^2 = F_{n-1} F_n - F_{n-2} F_{n-1}$$

$$(F_n)^2 = F_n F_{n+1} - F_{n-1} F_n$$

Somando ordenadamente todas essas n igualdades e simplificando, obtemos:

$$(F_1)^2 + (F_2)^2 + (F_3)^2 + \ldots + (F_{n-1})^2 + (F_n)^2 = F_n F_{n+1}$$

Assim, p.ex.:

$$1^2 + 1^2 + 2^2 + 3^2 + 5^2 + 8^2 + 13^2 =$$

$$= F_7F_8 = 13.21 = 273$$

Realmente:

$$1 + 1 + 4 + 9 + 25 + 64 + 169 = 273$$

17.5 IDENTIDADES ENTRE NÚMEROS DE FIBONACCI

(I) $F_{m+n} = F_{m-1}F_n + F_mF_{n+1}$

Demonstração:

Para cada valor de m usaremos o *"Teorema da indução matemática"* sobre n. A identidade subsiste para $n = 1$, pois, temos:

$$F_{m+1} = F_{m-1}F_1 + F_mF_2 = F_{m-1} + F_m$$

Suponhamos, agora, que a identidade subsiste para $n = 1,2, \ldots,k$, e demonstremos que também subsiste para $n = k + 1$. Então, temos (*hipótese de indução*):

$$F_{m+k} = F_{m-1}F_k + F_mF_{k+1}$$

$$F_{m+(k-1)} = F_{m-1}F_{k-1} + F_mF_k \quad .$$

Somando ordenadamente estas duas igualdades, obtemos:

$$F_{m+k} + F_{m+(k-1)} = F_{m-1}(F_k + F_{k-1}) + F_m(F_{k+1} + F_k)$$

ou seja:

$$F_{m+(k+1)} = F_{m-1}F_{k+1} + F_mF_{k+2}$$

que é precisamente a identidade (I) PARA $n = k + 1$. Logo, a identidade (I) subsiste para todos os valores inteiros e positivos de m e n.

Assim, p.ex.:

$$F_9 = F_{6+3} = F_5F_3 + F_6F_4 = 5.2 + 8.3 = 34$$

(II) $(F_{n+1})^2 = F_nF_{n+2} + (-1)^n$

Demonstração:

Usaremos o *"Teorema da indução matemática"*. A identidade subsiste para $n = 1$, pois, temos:

$$(F_2)^2 = 1^2 = 1.2 - 1 = F_1F_3 + (-1)$$

Suponhamos, agora, que a identidade *subsiste* para o inteiro positivo k *(hipótese de indução)*, isto é:

$$(F_{k+1})^2 = F_kF_{k+2} + (-1)^k$$

Somando aos dois membros o inteiro positivo $F_{k+1}F_{k+2}$, teremos, sucessivamente:

$$(F_{k+1})^2 + F_{k+1}F_{k+2} = F_kF_{k+2} + F_{k+1}F_{k+2} + (-1)^k$$

$$F_{k+1}(F_{k+1} + F_{k+2}) = F_{k+2}(F_k + F_{k+1}) + (-1)^k$$

$$F_{k+1}F_{k+3} = (F_{k+2})^2 + (-1)^k$$

$$(F_{k+2})^2 = F_{k+1}F_{k+3} + (-1)^{k+1}$$

isto é, a identidade (II) *subsiste* para o inteiro positivo k+1 e, portanto, *subsiste* para todo inteiro positivo n.

Assim, p.ex.:

$$(F_6)^2 = 8^2 = 13.5 - 1 = F_5F_7 + (-1)^5$$

$$(F_7)^2 = 13^2 = 21.8 + 1 = F_6F_8 + (-1)^6$$

17.6 PROPRIEDADES DOS NÚMEROS DE FIBONACCI

Teorema 17.6 Dois números de FIBONACCI *consecutivos* são *primos entre si*, isto é, o $mdc(F_n, F_{n+1}) = 1$ para todo inteiro $n \geq 1$.

Demonstração:

Determinando o $mdc(F_n, F_{n+1})$ pelo *algoritmo de EUCLIDES*,

temos:

$$F_{n+1} = 1.F_n + F_{n-1}$$

$$F_n = 1.F_{n-1} + F_{n-2}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$F_4 = 1.F_3 + F_2$$

$$F_3 = 2.F_2 + 0$$

Portanto:

$$\text{mdc}(F_n, F_{n+1}) = F_2 = 1$$

NOTA. Os números de FIBONACCI:

$$F_3 = 2, \quad F_5 = 5, \quad F_7 = 13, \quad F_{11} = 89$$

são todos *primos*, e por conseguinte é natural *conjecturar* que F_n é *primo para todo índice* $n > 2$ *que é primo*. Mas esta *conjectura* é *falsa*, porque F_{19} é um inteiro *composto:*

$$F_{19} = 4181 = 37.113$$

<u>Teorema 17.7</u> F_{mn} é *divisível* por F_m $(m,n \geq 1)$.

<u>Demonstração:</u>

Para cada valor de <u>m</u> usaremos o *"Teorema da indução matemá*

tica" sobre n. Como a proposição é verdadeira para $n=1$, suponhamos que F_{mn} é *divisível* por F_m para $n=1,2,\ldots,k$ *(hipótese de indução)*, e demonstremos que $F_{m(k+1)}$ é *divisível* por F_m. Temos, pela identidade (I):

$$F_{m(k+1)} = F_{mk+m} = F_{mk-1}F_m + F_{mk}F_{m+1}$$

Como F_m divide F_{mk-1} e F_{mk} *(hipótese de indução)*, segue-se que F_m divide o último membro das igualdades acima e, portanto, F_m divide $F_{m(k+1)}$. Logo, F_{mn} é divisível por F_m para os valores positivos de m e n.

LEMA. Se $m = nq + r$, então o

$$mdc(F_m,F_n) = mdc(F_n,F_r).$$

Demonstração:

Usando a identidade (I), temos:

$$mdc(F_m,F_n) = mdc(F_{nq+r}, F_n) = mdc(F_{nq-1}F_r + F_{nq}F_{r+1},F_n)$$

Mas, se $b|c$, o $mdc(a+c, b) = mdc(a,b)$, e como $F_n|F_{nq}$ (Teorema 17.7), segue-se que o

$$mdc(F_m,F_n) = mdc(F_{nq-1}F_r + F_{nq}F_{r+1},F_n) = mdc(F_{nq-1}F_r,F_n)$$

Posto isto, vamos demonstrar que o $mdc(F_{nq-1},F_n) = 1$. De fato, seja $d = mdc(F_{nq-1}, F_n)$. As relações:

$$d|F_n \quad e \quad F_n|F_{nq} \quad \text{implicam} \quad d|F_{nq}.$$

de modo que d é um divisor positivo comum dos números *consecutivos* F_{nq-1} e F_{nq} de FIBONACCI. Logo, pelo teorema 17.6, $d = 1$, isto é, o $mdc(F_{nq-1}, F_n) = d = 1$.

Finalmente, como o $mdc(a,c) = 1$ implica $mdc(a,bc) = mdc(a,b)$, temos:

$$mdc(F_m,F_n) = mdc(F_{nq-1}F_r,F_n) = mdc(F_n,F_r)$$

e a proposição fica demonstrada.

Teorema 17.8 O mdc de dois *números de FIBONACCI* também é um *número de FIBONACCI:*

$$mdc(F_m, F_n) = F_d, \quad \text{onde} \quad d = mdc(m,n)$$

Demonstração:

Suponhamos $m > n$. Determinando o $mdc(m,n)$ pelo *algoritmo de EUCLIDES*, obtemos as seguintes igualdades:

$$\begin{array}{ll}
m = nq_1 + r_1 , & 0 < r_1 < n \\
n = r_1q_2 + r_2 , & 0 < r_2 < r_1 \\
r_1 = r_2q_3 + r_3 , & 0 < r_3 < r_2 \\
\cdots\cdots\cdots\cdots & \\
r_{n-2} = r_{n-1}q_n + r_n, & 0 < r_n < r_{n-1} \\
r_{n-1} = r_nq_{n+1} + 0 &
\end{array}$$

Consoante o Lema anterior, temos:

$$mdc(F_m,F_n) = mdc(F_n,F_{r_1}) = mdc(F_{r_1},F_{r_2}) = \ldots = mdc(F_{r_{n-1}},F_{r_n})$$

Como $r_n | r_{n-1}$, segue-se que $F_{r_n} | F_{r_{n-1}}$ (Teorema 17.7) e, portanto o

$$mdc(F_{r_{n-1}}, F_{r_n}) = F_{r_n}$$

Mas, sendo r_n o último *resto* diferente de zero no *algoritmo de EUCLIDES*, o $mdc(m,n) = r_n$, o que implica:

$$mdc(F_m, F_n) = F_{mdc(m,n)}$$

e o teorema fica demonstrado.

Assim, p.ex.:

$$mdc(F_{16}, F_{12}) = F_{mdc(16,12)} = F_4 = 3$$

Realmente:

$$mdc(F_{16}, F_{12}) = mdc(987, 144) = 3$$

<u>Teorema 17.9</u> Se $F_m | F_n$, então $m | n$.

<u>Demonstração:</u>

Com efeito, se $F_m | F_n$, então o $mdc(F_m, F_n) = F_m$. Mas, pe-

lo teorema 17.8, o $mdc(F_m, F_n) = F_{mdc(m,n)}$. Assim sendo, o $mdc(m,n) = m$ e, portanto, $m|n$.

Note-se que este teorema é o *recíproco* do teorema 17.7, de modo que na sequência de FIBONACCI, $F_m|F_n$ *se e somente se* $m|n$.

EXERCÍCIOS

1. Determinar os *números de FIBONACCI:*

$$F_{15}, F_{18} \text{ e } F_{20}.$$

2. Calcular a soma dos 15 primeiros *números de FIBONACCI.*

3. Calcular a soma dos 12 primeiros *números de FIBONACCI* com *índices ímpares.*

4. Calcular a soma dos 10 primeiros *números de FIBONACCI* com *índices pares.*

5. Calcular a soma dos 17 primeiros *números de FIBONACCI* tomados alternadamente com os sinais + e −.

6. Calcular a soma dos quadrados dos 14 primeiros *números de FIBONACCI.*

7. Calcular o $mdc(F_{176}, F_{177})$ e o $mdc(F_{306}, F_{657})$.

8. Calcular o $mdc(F_{15}, F_{20})$ e o $mdc(F_{24}, F_{36})$.

9. Achar os *números de FIBONACCI* que dividem F_{24} e F_{36}.

10. Foi *conjecturado* que há somente *cinco números de FIBONACCI* que também são *números triangulares*. Achar esses *cinco números de FIBONACCI*.

11. Representar os inteiros 50, 75 e 100 como somas de distintos *números de FIBONACCI*.

12. Verificar que $5(F_n)^2 + 4(-1)^n$ é sempre um *quadrado perfeito* para $n = 1,2,\ldots,10$.

13. Demonstrar:

    (a) Se $2|F_n$, então $4|(F_{n+1}^2 - F_{n-1}^2)$

    (b) Se $3|F_n$, então $9|(F_{n+1}^3 - F_{n-1}^3)$

14. Demonstrar:

    (a) $F_{n+3} \equiv F_n \pmod{2}$, isto é, $F_3, F_6, F_9, \ldots$ são todos inteiros pares;

    (b) $F_{n+5} \equiv 3F_n \pmod{5}$, isto é, $F_5, F_{10}, F_{15}, \ldots$ são todos inteiros divisíveis por 5.

15. Levando em conta que $F_m | F_n$ se e somente se $m | n$, mostrar:

(a) $2 | F_n$ se e somente se $3 | n$;

(b) $3 | F_n$ se e somente se $4 | n$;

(c) $4 | F_n$ se e somente se $6 | n$;

(d) $5 | F_n$ se e somente se $5 | n$.

16. Demonstrar que, se o mdc$(m,n) = 1$, então

$$F_m F_n | F_{mn} \quad (m,n \geq 1).$$

17. Usando o *"Teorema da indução matemática"*, demonstrar:

$$F_1 + 2F_2 + 3F_3 + \ldots + nF_n = (n+1)F_{n+2} - F_{n+4} + 2$$

18. Demonstrar:

(a) $F_{2n-1} = (F_n)^2 + (F_{n-1})^2, \quad \forall\, n \geq 2$

(b) $F_{2n} = (F_{n+1})^2 - (F_{n-1})^2, \quad \forall\, n \geq 2$

(c) $F_n F_{n-1} = (F_n)^2 - (F_{n-1})^2 + (-1)^n, \quad \forall\, n \geq 2$

19. Demonstrar:

(a) $(F_{n+1})^2 - 4F_n F_{n-1} = (F_{n-2})^2, \quad \forall\, n \geq 3$

(b) $F_{n+1} F_{n-1} - F_{n+2} F_{n-2} = 2(-1)^n, \quad \forall\, n \geq 3$

(c) $(F_n)^2 - F_{n+2} F_{n-2} = (-1)^n, \quad \forall\, n \geq 3$

(d) $(F_n)^2 - F_{n+3} F_{n-3} = 4(-1)^{n+1}, \quad \forall\, n \geq 4$

(e) $F_n F_{n+1} F_{n+3} F_{n+4} = (F_n)^4 - 1, \quad \forall\, n \geq 1$

20. Demonstrar: $2^{n-1}F_n \equiv n \pmod{5}$, para todo inteiro $n \geqslant 1$.

21. Usando o *"Teorema da indução matemática"* demonstrar a *fórmula de BINET:*

$$F_n = (a^n - b^n)/\sqrt{5}$$

onde a e b são as raizes da equação quadrática $x^2 = x + 1$, isto é:

$$a = (1 + \sqrt{5})/2 \quad e \quad b = (1 - \sqrt{5})/2.$$

22. Demonstrar que, se r é o *resto* da divisão de F_n por F_m $(n > m)$, então r ou $F_m - r$ é um *número de FIBONACCI*. Exemplificar ambos os casos.

23. Demonstrar a identidade:

$$(F_n F_{n+3})^2 + (2F_{n+1}F_{n+2})^2 = (F_{2n+3})^2, \qquad \forall\, n \geqslant 1$$

24. Demonstrar a identidade:

$$\binom{n}{1}F_1 + \binom{n}{2}F_2 + \binom{n}{3}F_3 + \ldots + \binom{n}{n}F_n = F_{2n}, \qquad \forall\, n \geqslant 1$$

CAPÍTULO 18

TERNOS PITAGÓRICOS

18.1 CONCEITO DE TERNO PITAGÓRICO

<u>Definição 18.1</u> Chama-se *terno pitagórico* todo terno de inteiros positivos (a,b,c) tais que

$$a^2 + b^2 = c^2$$

Em outros termos, *terno pitagórico* é toda solução inteira e positiva da *equação diofantina:*

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

Assim, p.ex., são *ternos pitagóricos:*

(3,4,5), (6,8,10), (5,12,13), (12,35,37)

pois, temos:

$$3^2 + 4^2 = 5^2 \quad , \qquad 6^2 + 8^2 = 10^2$$

$$5^2 + 12^2 = 13^2 \quad , \qquad 12^2 + 35^2 = 37^2$$

Se (a,b,c) é um *terno pitagórico*, então (ka,kb,kc), onde $k > 1$ é um inteiro positivo qualquer, também é um *terno pitagórico*, pois, temos:

$$(ka)^2 + (kb)^2 = k^2a^2 + k^2b^2 = k^2(a^2 + b^2) =$$

$$= k^2c^2 = (kc)^2$$

18.2 FÓRMULAS QUE DÃO TERNOS PITAGÓRICOS

As fórmulas:

$$a = 2k + 1, \quad b = 2k^2 + 2k, \quad c = 2k^2 + 2k + 1$$

onde k é um inteiro positivo qualquer, atribuidas a PITÁGORAS, dão uma infinidade de *ternos pitagóricos*, pois, temos:

$$a^2 + b^2 = (2k + 1)^2 + (2k^2 + 2k)^2 =$$

$$= 4k^4 + 8k^3 + 8k^2 + 8k + 1 =$$

$$= (2k^2 + 2k + 1)^2 = c^2$$

Assim, p.ex., para $k = 7$, temos:

$$a = 2.7 + 1 = 15, \quad b = 2.7^2 + 2.7 = 112$$

$$c = 2.7^2 + 2.7 + 1 = 113$$

de modo que (15,112,113) é um *terno pitagórico*.

Analogamente, as fórmulas:

$$a = 2pq, \quad b = p^2 - q^2, \quad c = p^2 + q^2$$

onde p e q ($p > q$) são dois inteiros positivos quaisquer, atribuidas a PLATÃO, também dão uma infinidade de *ternos pitagóricos*, pois, temos:

$$a^2 + b^2 = (2pq)^2 + (p^2 - q^2)^2 = p^4 + 2p^2q^2 + q^4 =$$

$$= (p^2 + q^2)^2 = c^2$$

Assim, p.ex., para $p = 5$ e $q = 3$, temos:

$$a = 2.5.3 = 30, \quad b = 5^2 - 3^2 = 16$$

$$c = 5^2 + 3^2 = 34$$

de modo que (30,16,34) é um *término pitagórico*.

As fórmulas:

$$a = \frac{1}{2}(n^2 - 1), \quad b = n, \quad c = \frac{1}{2}(n^2 + 1)$$

fornecem *termos pitagóricos* mediante a substituição de n por um inteiro positivo *ímpar* maior do que 1.

Assim, p.ex., fazendo $n = 7$, temos:

$$a = \frac{1}{2}(7^2 - 1) = 24, \quad b = 7, \quad c = \frac{1}{2}(7^2 + 1) = 25$$

de modo que (24,7,25) é um *termo pitagórico*.

É imediato que a todo *terno pitagórico* (a,b,c) está *associado* um *triângulo retângulo* cujas medidas respectivas dos *catetos* e da *hipotenusa* são a, b e c, denominado *triângulo pitagórico*.

18.3 TERNOS PITAGÓRICOS PRIMITIVOS

Definição 18.2 Chama-se *terno pitagórico primitivo* todo terno pitagórico (a,b,c) tal que o mdc(a,b) = 1.

Em outros termos, *terno pitagórico primitivo* é todo terno pitagórico (a,b,c) em que os inteiros positivos a e b são *primos entre si*.

Assim, p.ex., são *ternos pitagóricos primitivos:*

$$(5,12,13), \quad (8,15,17), \quad (9,40,41)$$

pois, são ternos pitagóricos nos quais o

$$\text{mdc}(5,12) = \text{mdc}(8,15) = \text{mdc}(9,40) = 1.$$

Note-se que, se (a,b,c) é um *terno pitagórico primitivo*, isto é:

$$a^2 + b^2 = c^2 \quad \text{e o mdc}(a,b) = 1$$

então, se tem:

$$\text{mdc}(a,c) = \text{mdc}(b,c) = \text{mdc}(a,b,c) = 1$$

porque todo divisor d de dois quaisquer dos três inteiros positivos a, b, c divide também o terceiro.

Se (a,b,c) é um terno pitagórico *não primitivo*, isto é, tal que o $mdc(a,b) = d \neq 1$, então $d|c$, e os quocientes:

$$a_1 = a/d, \quad b_1 = b/d, \quad c_1 = c/d$$

formam o *terno pitagórico primitivo* (a_1,b_1,c_1), pois, temos:

$$a_1^2 + b_1^2 = (\frac{a}{d})^2 + (\frac{b}{d})^2 = \frac{a^2 + b^2}{d^2} = \frac{c^2}{d^2} = (\frac{c}{d})^2 = c_1^2$$

e o $mdc(a_1,b_1) = 1$.

Portanto, qualquer terno pitagórico *não primitivo* se pode obter de um *terno pitagórico primitivo* multiplicando-se os seus elementos por um *conveniente* inteiro positivo maior do que 1, isto é, todas as soluções de $x^2 + y^2 = z^2$ resultam daquelas de $x_1^2 + y_1^2 = z_1^2$, onde o $mdc(x_1,y_1) = 1$.

Assim, p.ex., os ternos pitagóricos *não primitivos:*

(15,36,39) e (25,60,65)

resultam ambos do *terno pitagórico primitivo* (5,12,13) multiplicando-se os elementos deste respectivamente pelos inteiros 3 e 5.

NOTA. Com todos os elementos menores que 1000 são conhecidos 158 *termos pitagóricos primitivos*, e aquele que tem os maiores elementos é (372,925,997).

18.4 PROPRIEDADES DOS TERNOS PITAGÓRICOS

Teorema 18.1 Para todo inteiro positivo $a > 2$ existem inteiros positivos b e c tais que (a,b,c) é um *terno pitagórico*.

Demonstração:

Suponhamos, primeiro, que o inteiro $a > 2$ é *par*. Então, $2|a$ e $4|a^2$, de modo que

$$b = (a^2 - 4)/4 \quad \text{e} \quad c = (a^2 + 4)/4$$

são dois inteiros positivos. E como

$$a^2 + b^2 = a^2 + \frac{a^4 - 8a^2 + 16}{16} = \left(\frac{a^2 + 4}{4}\right)^2 = c^2$$

segue-se que (a,b,c) é um *terno pitagórico*.

Suponhamos, agora, que o inteiro $a > 2$ é ímpar. Então, $a = 2k + 1$ e as *fórmulas de PITÁGORAS:*

$$a = 2k + 1, \quad b = 2k^2 + 2k, \quad c = 2k^2 + 2k + 1$$

onde k é um inteiro positivo qualquer, dão o *terno pitagórico* (a,b,c).

Teorema 18.2 Um terno (a,b,c) é um *terno pitagórico* se e somente se existem inteiros u e v que verificam as seguintes condições:

(i) $u > v > 0$

(ii) $u \equiv v \pmod{2}$

(iii) uv é um *quadrado perfeito*

(iv) $a = \sqrt{uv}, \quad b = (u - v)/2, \quad c = (u + v)/2$

Demonstração:

($\Longrightarrow$) Suponhamos, primeiro, que u e v são dois inteiros que verificam as quatro condições enumeradas no enunciado do teorema. Então, por (i) e (iv), a, b e c são *positivos*, por (iii) e (iv), a é um *inteiro*, e por (ii) e (iv), b e c também são *inteiros* (a condição (ii) é um modo abreviado de dizer que os inteiros u e v são ambos *pares* ou ambos *ímpares*). Finalmente, pela (iv), temos:

$$a^2 + b^2 = uv + \frac{u^2 - 2uv + v^2}{4} = \left(\frac{u + v}{2}\right)^2 = c^2$$

e, portanto, (a,b,c) é um *terno pitagórico*.

($\Longleftarrow$) Reciprocamente, suponhamos, agora, que (a,b,c) é um *terno pitagórico*. Cumpre achar inteiros $\underline{u}$ e $\underline{v}$ que verifiquem as quatro condições enumeradas no enunciado do teorema. Seja

$$u = c + b \quad e \quad v = c - b$$

Como $\underline{b}$ e $\underline{c}$ são inteiros positivos e $c > b$, temos $u > v > 0$, de modo que (i) é satisfeita.

Por ser $u - v = 2b$, segue-se que $2 \mid (u - v)$, isto é:

$$u \equiv v \pmod{2}$$

e a condição (ii) é satisfeita.

A condição (iii) é satisfeita, pois, temos:

$$uv = (c + b)(c - b) = c^2 - b^2 = a^2$$

Finalmente, a condição (iv) também é satisfeita, pois, temos:

$$\sqrt{uv} = a, \quad (u - v)/2 = 2b/2 = b, \quad (u + v)/2 = 2c/2 = c$$

<u>Exemplo 18.1</u> Mostrar que $(360, 319, 481)$ é um *terno pitagórico*.

Os inteiros:

$$u = 481 + 319 = 800, \quad v = 481 - 319 = 162$$

satisfazem as quatro condições enumeradas no enunciado do teorema 18.2:

(i) $u > v > 0$, porque $800 > 162 > 0$

(ii) $u \equiv v \pmod{2}$, porque $u - v = 638$ e $2 | 638$

(iii) $uv = 129600 = 360^2$, *quadrado perfeito*

(iv) $\sqrt{uv} = 360$, $(u - v)/2 = 638/2 = 319$

$(u + v)/2 = 962/2 = 481$

Logo, (360, 319, 481) é um *terno pitagórico*.

<u>Teorema 18.3</u> Se (a,b,c) é um *terno pitagórico primitivo*, então <u>c</u> é *ímpar* e $a \not\equiv b \pmod{2}$.

<u>Demonstração:</u>

Se $a \equiv b \pmod{2}$, então <u>a</u> e <u>b</u> são ambos *pares* ou são ambos *ímpares*. Se <u>a</u> e <u>b</u> são ambos *pares*, então $2 | mdc(a,b)$, o que é *impossível*, porque o $mdc(a,b) = 1$. E se, ao invés, <u>a</u> e <u>b</u> são ambos *ímpares*, então $c^2 = a^2 + b^2$ é *par* e, portanto, <u>c</u> é *par*, isto é, se $a = 2h + 1$ e $b = 2k+1$, então $c = 2n$, e temos:

$$a^2 = 4h^2 + 4h + 1 \equiv 1 \pmod{4}$$

$$b^2 = 4k^2 + 4k + 1 \equiv 1 \pmod{4}$$

$$c^2 = 4n^2 \equiv 0 \pmod{4}$$

o que implica:

$$a^2 + b^2 \equiv 2 \pmod{4}$$

ou seja:

$$c^2 = a^2 + b^2 \equiv 2 \pmod{4}$$

e, portanto, $2 \equiv 0 \pmod{4}$, o que é *absurdo*. Assim sendo, só pode ser $a \not\equiv b \pmod{2}$, de modo que a e b são de *paridade* diferente, e como $a^2 + b^2 = c^2$, segue-se que c^2 é *ímpar*, o que implica c também *ímpar*.

NOTA. De conformidade com este teorema, num *termo pitagórico primitivo* qualquer (a,b,c), há exatamente *um* elemento que é *par* (a ou b) e *dois* elementos que são *ímpares* (a e c ou b e c), de modo que a soma $a + b + c$ é sempre um inteiro positivo *par*.

EXERCÍCIOS

1. Achar os *termos pitagóricos* dados pelas *fórmulas de PITÁGORAS* para $k = 3,5,8$.

2. Achar os *termos pitagóricos* dados pelas *fórmulas de PLATÃO* para os seguintes pares de valores de p e q:

   (a) $p = 6$ e $q = 4$; (b) $p = 9$ e $q = 7$

3. O *terno pitagórico* (19,b,c) é dado pelas *fórmulas de PITÁGORAS*. Determinar b e c.

4. O *terno pitagórico* (20,b,c) é dado pelas fórmulas de PLATÃO. Determinar b e c.

5. Construir três *ternos pitagóricos* (a,b,c) tais que os elementos b e c sejam inteiros consecutivos.

6. Achar três *ternos pitagóricos* distintos da forma (16,b,c).

7. Achar todos os *ternos pitagóricos* da forma (a,30,c).

8. Achar todos os *ternos pitagóricos primitivos* da forma (40,b,c).

9. Achar todos os *ternos pitagóricos primitivos* da forma (60,b,c).

10. Mostrar que (3,4,5) é o *único terno pitagórico primitivo* formado por inteiros positivos consecutivos.

11. Demonstrar que num *terno pitagórico primitivo* (a,b,c) o produto ab é divisível por 12 e o produto abc é divisível por 60.

12. Demonstrar que, se $n \not\equiv$ (mod.4), então existe um *terno pitagórico primitivo* (x,y,z) no qual x=n ou y=n.

13. Mostrar que (3n,4n,5n),onde n=1,2,3,...,são os *únicos*

ternos pitagóricos cujos elementos estão em *progressão aritmética.*

14. Demonstrar que, se (a,b,c) é um *terno pitagórico primitivo*, então a ou b é divisível por 3.

15. Mostrar que, se a é um inteiro positivo *ímpar*, então existe um terno pitagórico (a,b,c) tal que c=b+1.

16. Demonstrar que num *terno pitagórico* (a,b,c):
    (a) Um dos elementos a, b ou c é divisível por 5.
    (b) a, b, a+b ou a-b é divisível por 7.

17. Seja (a,b,c) um *terno pitagórico primitivo* no qual b é *ímpar*. Mostrar que $4|a$.

18. Seja (a,b,c) um *terno pitagórico*. Mostrar:

$$\frac{c+b}{a} = \sqrt{\frac{c+b}{c-b}}$$

19. Mostrar que o *número* de *ternos pitagóricos* (x,y,z) cujo primeiro elemento x = a, sendo a um inteiro positivo dado, é igual a

$$(d(a^2) - 1)/2 \quad \text{se } a \text{ é } \textit{ímpar}$$

$$(d(a^2/4) - 1)/2 \quad \text{se } a \text{ é } \textit{par}$$

CAPÍTULO 19

CLASSES RESIDUAIS

19.1 CONCEITO DE CLASSE RESIDUAL

Definição 19.1 Chama-se *classe residual módulo* m de um inteiro a o conjunto de todos os inteiros que são *congruentes* a *a módulo* m.

Este conjunto representa-se por a_m. Portanto, simbolicamente:

$$a_m = \{ x \in Z \mid x \equiv a \ (\text{mod.}m) \} =$$

$$= \{ x \in Z \mid m | (x - a) \}$$

ou seja:

$$a_m = \{ x \mid x = a + km, \ k \in Z \}$$

Em particular, se o *módulo* $m = 1$, então:

$$a_1 = \{ x \in Z \mid 1 | (x - a) \} = Z$$

isto é, a *classe residual módulo* 1 de um inteiro qualquer $\underline{a}$ é o conjunto Z dos inteiros.

As *classes residuais módulo* $\underline{m}$ também são denominadas *inteiros módulo* $\underline{m}$.

Note-se que $a \equiv a \pmod{m}$, porque $m|0$, de modo que $a \in a_m$, isto é, a *classe residual módulo* $\underline{m}$ *de qualquer inteiro* $\underline{a}$ *nunca é vazia:* $a_m \neq \phi$ para todo $a \in Z$.

<u>Exemplo 19.1</u> A *classe residual módulo* 3 *do inteiro* 2 é o conjunto:

$$2_3 = \{ 3 \mid x = 2 + 3k, \quad k \in Z \} =$$

$$= \{ \ldots, -7, -4, -1, 2, 5, 8, 11, \ldots \}$$

Observe-se que

$$2_3 = (-7)_3 = 11_3 = 35_3 = \ldots$$

isto é, os símbolos distintos $(-7)_3$, 2_3, 11_3, 35_3, ... designam todos um mesmo conjunto - *a classe residual módulo* 3 *do inteiro* 2.

<u>Exemplo 19.2</u> A *classe residual módulo* 5 *do inteiro* -4 é o conjunto:

$$(-4)_5 = \{ x \mid x = -4 + 5k, \quad k \in Z \} =$$

$$= \{ \ldots, -19, -14, -9, -4, 1, 6, 11, \ldots \}$$

Observe-se que

$$(-4)_5 = 1_5 = 6_5 = 11_5 = \ldots$$

19.2 PROPRIEDADES DAS CLASSES RESIDUAIS

Sejam a_m e b_m as *classes residuais módulo* $\underline{m}$ de dois inteiros quaisquer $\underline{a}$ e $\underline{b}$.

Teorema 19.1 As classes residuais a_m e b_m são *iguais* se e somente se $a \equiv b \pmod{m}$.

Demonstração:

($\Longrightarrow$) Suponhamos que $a \equiv b \pmod{m}$, e seja $\underline{x}$ um elemento *qualquer* de $a_m (x \in a_m)$. Então:

$$x \equiv a \pmod{m} \quad e \quad a \equiv b \pmod{m} \Longrightarrow x \equiv b \pmod{m}$$

e isto significa que $x \in b_m$. Logo: $a_m \subset b_m$ (1).

Seja, agora $\underline{y}$ um elemento *qualquer* de $b_m (y \in b_m)$. Então:

$$y \equiv b \pmod{m} \quad e \quad a \equiv b \pmod{m} \Longrightarrow y \equiv a \pmod{m}$$

e isto significa que $y \in a_m$. Logo: $b_m \in a_m$ (2).

Das *inclusões* (1) e (2), resulta: $a_m = b_m$.

($\Longleftarrow$) Reciprocamente, suponhamos que $a_m = b_m$. Como $a \in a_m$, segue-se que $a \in b_m$ e, portanto: $a \equiv b \pmod{m}$.

<u>Teorema 19.2</u> Se as classes residuais a_m e b_m *não são disjuntas* ($a_m \cap b_m \neq \phi$), então *coincidem:* $a_m = b_m$.

<u>Demonstração:</u>

Com efeito, se a_m e b_m *não são disjuntas*, então existe ao menos um inteiro <u>c</u> tal que $c \in a_m$ e $c \in b_m$, isto é, tal que

$$c \equiv a \pmod{m} \quad e \quad c \equiv b \pmod{m} \Longrightarrow a \equiv b \pmod{m}$$

Logo, pelo teorema 19.1: $a_m = b_m$.

<u>Teorema 19.3</u> Se as classes residuais a_m e b_m são *distintas* ($a_m \neq b_m$), então são *disjuntas:* $a_m \cap b_m = \phi$.

<u>Demonstração:</u>

Com efeito, se a_m e b_m *não são disjuntas*, então existe um inteiro <u>c</u> tal que $c \in a_m$ e $c \in b_m$, isto é, tal que

$$c \equiv a \pmod{m} \quad e \quad c \equiv b \pmod{m} \Longrightarrow a \equiv b \pmod{m}$$

Logo, pelo teorema 19.1: $a_m = b_m$, o que é *impossível*, visto que, por hipótese, $a_m \neq b_m$.

NOTA: A classe residual a_m diz-se *determinada* ou *definida* pelo inteiro $\underline{a}$, o qual, por sua vez, chama-se um *representante* de a_m.

Dois inteiros são representantes de uma mesma *classe residual módulo* $\underline{m}$ se e somente se são *congruentes módulo* $\underline{m}$.

19.3 CONJUNTO DAS CLASSES RESIDUAIS

O conjunto de todas as *classes residuais módulo* $\underline{m}$ indica se por Z_m, isto é, simbolicamente:

$$Z_m = \{ a_m \mid a \in Z \}$$

Em particular, se o módulo $m = 1$, então $a_1 = Z$ para todo $a \in Z$, de modo que $Z_1 = \{Z\}$.

Note-se que, na Teoria dos Conjuntos, Z_m outra coisa não é que o *conjunto-quociente* de Z pela *congruência módulo* $\underline{m}$

<u>Teorema 19.4</u> O conjunto Z_m encerra $\underline{m}$ *classes residuais módulo* $\underline{m}$ *distintas*.

<u>Demonstração:</u>

(i) As classes residuais módulo $\underline{m}$ dos inteiros $\underline{x}$ que satisfazem à condição $x \in [0, m-1]$ são todas *distin-*

tas, porque, se a e b são dois inteiros tais que $a,b \in [0,m-1]$, então:

$$|a - b| < m \implies a \not\equiv b \ (\text{mod.}m) \implies a_m \neq b_m$$

(ii) Por outra parte, dado um inteiro qualquer

$$y \in [0, m-1],$$

temos, pelo algoritmo da divisão:

$$y - r = mq, \quad \text{com} \quad 0 \leqslant r < m$$

o que implica:

$$y \equiv r \ (\text{mod.}m) \implies y_m = r_m, \quad \text{com} \quad r \in [0, m-1]$$

(iii) Como existem apenas m inteiros $x \in [0,m-1]$, que são: $0,1,2,\ldots,m-1$, segue-se que o conjunto Z_m encerra m classes residuais módulo m *distintas:*

$$Z_m = \{0_m, 1_m, 2_m, \ldots, (m-1)_m\}$$

Observe-se que Z_m é um conjunto *finito*, embora Z não o seja.

NOTA. Para achar a *classe residual módulo* m de um inteiro qualquer y basta determinar o *resto* r da divisão de y por m, pois, temos $y_m = r_m$, com $0 \leqslant r < m$, conforme mostra a demonstração do teorema 19.4. Portanto, a *classe resi-*

dual módulo m de qualquer inteiro é igual à *classe residual módulo* m de um inteiro não negativo menor que m.

Assim, p.ex., seja achar a *classe residual módulo* 8 *de* 75. Como 75 = 8.9 + 3, temos:

$$75 \equiv 3 \ (\text{mod.}8) \Longrightarrow 75_8 = 3_8 =$$

$$= \{ x \mid x = 3 + 8k, \quad k \in Z \} =$$

$$= \{ \ldots, -13, -5, 3, 11, 19, \ldots \}$$

Exemplo 19.3 Se o *módulo* m = 2, temos *duas* classes residuais módulo 2 *distintas:*

$$0_2 = \{ x \mid x = 0 + 2k, \quad k \in Z \} =$$

$$= \{ \ldots, -6, -4, -2, 0, 2, 4, 6, \ldots \}$$

$$= (-4)_2 = 4_2 = 8_2 = \ldots$$

$$1_2 = \{ x \mid x = 1 + 2k, \quad k \in Z \} =$$

$$= \{ \ldots, -5, -3, -1, 1, 3, 5, \ldots \} =$$

$$= (-3)_2 = 5_2 = 7_2 = \ldots$$

A classe residual 0_2 é formada por todos os inteiros *pares* e a classe residual 1_2 é formada por todos os inteiros *ímpares*. Portanto:

$$Z_2 = \{ 0_2, 1_2 \}$$

Note-se que $0_2 \cap 1_2 = \phi$ e $0_2 \cup 1_2 = Z$.

<u>Exemplo 19.4</u> Se o *módulo* m = 5, temos *cinco* classes residuais módulo 5 *distintas:*

$$0_5 = \{ x \mid x = 0 + 5k, \quad k \in Z \} =$$

$$= \{ \ldots, -15, -10, -5, 0, 5, 10, 15, \ldots \} =$$

$$= (-10)_5 = 5_5 = 15_5 = \ldots$$

$$1_5 = \{ x \mid x = 1 + 5k, \quad k \in Z \} =$$

$$= \{ \ldots, -14, -9, -4, 1, 6, 11, 16, \ldots \} =$$

$$= (-9)_5 = 6_5 = 21_5 = \ldots$$

$$2_5 = \{ x \mid x = 2 + 5k, \quad k \in Z \} =$$

$$= \{ \ldots, -13, -8, -3, 2, 7, 12, 17, \ldots \} =$$

$$= (-3)_5 = 2_5 = 17_5 = \ldots$$

$$3_5 = \{ x \mid x = 3 + 5k, \quad k \in Z \} =$$

$$= \{ \ldots, -12, -7, -2, 3, 8, 13, 18, \ldots \} =$$

$$= (-7)_5 = 8_5 = 23_5 = \ldots$$

$$4_5 = \{ x \mid x = 4 + 5k, \quad k \in Z \} =$$

$$= \{ \ldots, -11, -6, -1, 4, 9, 14, 19, \ldots \} =$$

$$= (-11)_5 = 4_5 = 19_5 = \ldots$$

Portanto:

$$Z_5 = \{ 0_5, 1_5, 2_5, 3_5, 4_5 \}$$

Esta representação de Z_5 *não é única*, pois, temos:

$$Z_5 = \{ 5_5, (-4)_5, 7_5, (-2)_5, 9_5 \}$$

Note-se:-

$$0_5 \cap 1_5 \cap 2_5 \cap 3_5 \cap 4_5 = \phi \quad \text{e} \quad 0_5 \cup 1_5 \cup 2_5 \cup 3_5 \cup 4_5 = Z.$$

NOTA. Em cada um destes dois exemplos observe-se que as classes residuais obtidas possuem as três seguintes propriedades: (1) *não são vazias*; (2) *são disjuntas duas a duas*; (3) *sua renião* é o conjunto Z dos inteiros. Exprime-se este fato dizendo que os conjuntos Z_2 e Z_5 são *partições* do conjunto Z dos inteiros.

De modo geral, as m classes residuais 0_m, 1_m, 2_m, ..., $(m-1)_m$ que formam o conjunto Z_m possuem estas mesmas três propriedades, de modo que o conjunto Z_m é uma *partição* do conjunto Z dos inteiros.

Importa ainda notar que um conjunto de m *representantes*,

um de cada uma das classes residuais $0_m, 1_m, 2_m, \ldots, (m-1)_m$, é um *sistema completo de restos módulo* $\underline{m}$.

Assim, p.ex., o conjunto:

$$\{-5, 11, -8, 13, -6\}$$

é um *sistema completo de restos módulo* 5.

EXERCÍCIOS

1. Achar a *classe residual módulo* 8 de -5.

2. Achar a *classe residual módulo* 9 de 1913.

3. O inteiro 17 pertence à classe residual módulo $\underline{m}$ de 24. Determinar $\underline{m}$.

4. Os inteiros 29 e 41 pertencem a uma mesma classe residual módulo $\underline{m}$. Determinar $\underline{m}$.

5. Mostrar: $10_3 = 1_3$, $84_{19} = 8_{19}$, $(-8)_7 = 20_7$.

CAPÍTULO 20

REPRESENTAÇÃO DOS INTEIROS EM OUTRAS BASES. CRITÉRIOS DE DIVISIBILIDADE

20.1 REPRESENTAÇÃO DOS INTEIROS EM OUTRAS BASES

Teorema 20.1 Dado um inteiro qualquer $b \geqslant 2$, todo inteiro positivo n admite uma *única representação* da forma:

$$n = a_m b^m + a_{m-1} b^{m-1} + \ldots + a_2 b^2 + a_1 b + a_o$$

onde os a_i são tais que $0 \leqslant a_i < b$, $i = 0,1,2,\ldots,m$.

Demonstração:

Pelo algoritmo da divisão aplicado aos inteiros n e b, temos:

$$n = bq_1 + a_o, \quad 0 \leqslant a_o < b \qquad (0)$$

Aplicando, agora, o algoritmo da divisão ao quociente q_1 e ao inteiro b, temos:

$$q_1 = bq_2 + a_1, \quad 0 \leqslant a_1 < b \qquad (1)$$

Analogamente, continuando a aplicar o algoritmo da divisao aos quocientes obtidos q_i e ao inteiro b, temos:

$$q_2 = bq_3 + a_2, \quad 0 \leqslant a_2 < b \qquad (2)$$

$$q_3 = bq_4 + a_3, \quad 0 \leqslant a_3 < b \qquad (3)$$

e assim por diante.

Como $n > q_1 > q_2 > q_3 > \ldots$ e cada $q_i \geqslant 0$, esta sequência decrescente dos quocientes q_i é *finita*, isto é, existe um índice m tal que

$$q_{m-1} = bq_m + a_{m-1}, \quad 0 \leqslant a_{m-1} < b \qquad (m-1)$$

$$q_m = b.0 + a_m = a_m, \quad 0 < a_m < b \qquad (m)$$

Multiplicando por b ambos os membros de (1), por b^2 ambos os membros de (2), por b^3 ambos os membros de (3),... ..., por b^{m-1} ambos os membros de (m-1), obtemos o conjunto de igualdades:

$$n = bq_1 + a_o, \quad 0 \leqslant a_o < b$$

$$bq_1 = b^2q_2 + a_1b, \quad 0 \leqslant a_1 < b$$

$$b^2q_2 = b^3q_3 + a_2b^2, \quad 0 \leqslant a_2 < b$$

$$b^3q_3 = b^4q_4 + a_3b^3, \quad 0 \leqslant a_3 < b$$

$$\ldots\ldots\ldots\ldots\ldots\ldots \qquad \ldots\ldots\ldots$$

$$b^{m-1}q_{m-1} = b^m a_m + a_{m-1}b^{m-1}, \quad 0 \leqslant a_{m-1} < b$$

Somando ordenadamente todas essas m igualdades, teremos:

$$n + (bq_1 + b^2q_2 + \ldots + b^{m-1}q_{m-1}) =$$

$$= (bq_1 + b^2q_2 + \ldots + b^{m-1}q_{m-1}) +$$

$$+ a_o + a_1b + a_2b^2 + \ldots + a_{m-1}b^{m-1} + a_mb_m$$

ou, finalmente:

$$n = a_mb^m + a_{m-1}b^{m-1} + \ldots + a_2b^2 + a_1b + a_o$$

Assim, dado um inteiro qualquer $b \geqslant 2$, todo inteiro positivo n pode ser representado por um *polinômio inteiro em b* do *grau m* (porque $a_m \neq 0$), *ordenado segundo as potências decrescentes de b*, e cujos *coeficientes* a_i são inteiros que satisfazem às condições:

$$0 \leqslant a_i < b \ (i = 0,1,2,\ldots,m), \quad \text{sendo} \quad a_m \neq 0$$

Este polinômio representa-se, de modo abreviado, pela notação:

$$n = (a_ma_{m-1}\ldots a_2a_1a_o)_b$$

em que os coeficientes a_i são indicados pela *ordem* respectiva, figurando o inteiro b como um *índice*.

A *unicidade* desta representação é uma consequência imediata do teorema 4.2.

O inteiro b chama-se *base* e é costume dizer que n está escrito no *sistema de base* b.

Assim, p.ex.:

$$105 = 1.2^6 + 1.2^5 + 0.2^4 + 1.2^3 + 0.2^2 + 0.2 + 1$$

ou, sob forma abreviada:

$$105 = (1101001)_2$$

Por outro lado, temos:

$$(100111)_2 = 1.2^5 + 0.2^4 + 0.2^3 + 1.2^2 + 1.2 + 1 = 39$$

Exemplo 20.1 Escrever 31415 no sistema de *base* 8.

Temos, sucessivamente:

$$31415 = 8.3926 + 7$$
$$3926 = 8.490 + 6$$
$$490 = 8.61 + 2$$
$$61 = 8.7 + 5$$
$$7 = 8.0 + 7$$

Portanto:

$$31415 = 7.8^4 + 5.8^3 + 2.8^2 + 6.8 + 7 = (75267)_8$$

Exemplo 20.2 Escrever $(3531)_6$ no sistema de *base* 10.

Temos:

$$(3531)_6 = 3.6^3 + 5.6^2 + 3.6 + 1 = 3.216 + 5.36 + 3.6 + 1 =$$

$$= 648 + 180 + 18 + 1 = 847$$

Exemplo 20.3 Escrever $(6165)_7$ no sistema de *base* 12.

Temos:

$$(6165)_7 = 6.7^3 + 1.7^2 + 6.7 + 5 = 6.343 + 1.49 + 6.7 + 5 =$$

$$= 2058 + 49 + 42 + 5 = 2154.$$

Cumpre, agora, escrever 2154 (base 10) no sistema de *base* 12. Temos, sucessivamente:

$$2154 = 12.179 + 6$$
$$179 = 12.14 + 11$$
$$14 = 12.1 + 2$$
$$1 = 12.0 + 1$$

No sistema de *base* 12 é habitual denotar 10 e 11 por a e b, respectivamente, de modo que os *algarismos* deste sistema são 0,1,2,3,4,5,6,7,8,9,a,b.

Portanto:

$$2154 = 1.12^3 + 2.12^2 + b.12 + 6 = (12b6)_{12}$$

20.2 CRITÉRIOS DE DIVISIBILIDADE

Definição 20.1 Chama-se *critério de divisibilidade* todo conjunto de condições que permitem reconhecer se um inteiro dado é *divisível* por outro.

Assim, p.ex., um inteiro n é *divisível por* 2 se n é *par*. E como n é *par* se o algarismo das unidades de n é *par*, segue-se que o *critério de divisibilidade por* 2 é que o algarismo das unidades do inteiro dado seja 0, 2, 4, 6 ou 8.

Todo inteiro positivo n pode ser expresso sob a forma $10k + r$, onde r é um inteiro tal que $0 \leqslant r < 10$, de modo que n é divisível por 5 se $10k + r$ é divisível por 5, isto é, se $r = 0$ ou $r = 5$. E como r representa o algarismo das unidades de n, segue-se que o *critério de divisibilidade por* 5 é que o algarismo das unidades do inteiro dado seja 0 ou 5.

As propriedades da relação de congruência permitem estabelecer critérios especiais de divisibilidade de um inteiro dado por outro, mas muitos deles são de difícil aplicação e, portanto, carecem de utilidade prática.

Lema 20.1 Se $a \equiv b \pmod{m}$ e se

$$P(x) = \sum_{k=0}^{n} c_k x^k = c_o + c_1 x + c_2 x^2 + \ldots + c_n x^n$$

é um polinômio em $\underline{x}$ com coeficientes c_k inteiros, então:

$$P(a) \equiv P(b) \pmod{m}$$

Demonstração:

Por ser $a \equiv b \pmod{m}$, temos (Teorema 9.4):

$$a^k \equiv b^k \pmod{m}, \quad \text{para} \quad k = 0,1,2,\ldots,n$$

e, portanto:

$$c^k a^k \equiv c^k b^k \pmod{m}, \text{ para } k = 0,1,2,\ldots,n$$

Somando ordenadamente todas essas $n+1$ congruências, obtemos:

$$\sum_{k=0}^{n} c_k a^k \equiv \sum_{k=0}^{n} c_k b^k \pmod{m}$$

ou seja:

$$P(a) \equiv P(b) \pmod{m}$$

Se $P(a) \equiv 0 \pmod{m}$, diz-se que $\underline{a}$ é uma *solução* da congruência $P(x) \equiv 0 \pmod{m}$.

Corolário 20.1 Se $\underline{a}$ é uma *solução* da congruência $P(x) \equiv 0 \pmod{m}$ e se $a \equiv b \pmod{m}$, então $\underline{b}$ também é uma *solução* desta congruência.

Demonstração:

Com efeito, pela proposição anterior, temos

$$P(a) \equiv P(b) \pmod{m}.$$

Portanto, se a é uma *solução* de $P(x) \equiv 0 \pmod{m}$, então:

$$P(b) \equiv P(a) \equiv 0 \pmod{m}$$

de modo que b também é uma *solução* de $P(x) \equiv 0 \pmod{m}$.

20.3 CRITÉRIO DE DIVISIBILIDADE POR 9

Teorema 20.2 Seja

$$n = a_m.10^m + a_{m-1}.10^{m-1} + \ldots + a_1.10 + a_o$$

a representação no sistema decimal (base 10) do inteiro positivo n, onde cada a_k é um inteiro tal que $0 \leq a_k < 10$, e seja S a soma dos seus algarismos:

$$S = a_o + a_1 + \ldots + a_{m-1} + a_m$$

Então, o inteiro positivo n é divisível por 9 $(9|n)$ se e somente se S é divisível por 9 $(9|S)$.

Demonstração:

Consideremos o polinômio em x com coeficientes inteiros:

$$P(x) = \sum_{k=0}^{m} a_k x^k$$

Por ser $10 \equiv 1 \pmod{9}$, temos (lema 20.1):

$$P(10) \equiv P(1) \pmod{9}$$

Como $P(10) = n$ e $P(1) = S$, segue-se que $n \equiv S \pmod{9}$. Assim sendo $n \equiv 0 \pmod{9}$ se e somente se $S \equiv 0 \pmod{9}$, isto é, $9|n$ se e somente se $9|S$.

Assim, p.ex., o inteiro $n = 26356734$ é *divisível por* 9, porque a soma dos seus algarismos é

$$S = 2 + 6 + 3 + 5 + 6 + 7 + 3 + 4 = 36$$

e 36 é divisível por 9. Realmente:

$$26356734 = 9 \times 2928526.$$

<u>Exemplo 20.4</u> Determinar os algarismos <u>x</u> e <u>y</u> do inteiro $n = 75x4y$ de modo que <u>n</u> seja divisível por 5 e por 9.

Pelo critério de divisibilidade por 5 só pode ser $y = 0$ ou $y = 5$, e pelo critério de divisibilidade por 9 deve ser:

$$7 + 5 + x + 4 + y \equiv 0 \pmod{9}$$

ou

$$x + y \equiv -16 \equiv 2 \pmod{9}$$

Como <u>x</u> e <u>y</u> são ambos menores que 10, só pode ser:

$$x + y = 2 \quad \text{ou} \quad x + y = 11$$

Se $y = 0$, então $x = 2$ ou $x = 11$ (impossível), o que dá o inteiro 75240, e se $y = 5$, então $x = -3$ (impossível) ou $x = 6$, o que dá o inteiro 75645, isto é, o problema admite duas soluções.

20.4 CRITÉRIO DE DIVISIBILIDADE POR 11

Teorema 20.3 Seja

$$n = a_m.10^m + a_{m-1}.10^{m-1} + \ldots + a_1.10 + a_o$$

a representação no sistema decimal (base 10) do inteiro positivo n, onde cada a_k é um inteiro tal que $0 \leqslant a_k < 10$, e seja

$$T = a_o - a_1 + a_2 - \ldots + (-1)^m a_m$$

Então, o inteiro positivo n é divisível por 11 ($11|n$) se e somente se T é divisível por 11 ($11|T$).

Demonstração:

Consideremos o polinômio em x com coeficientes inteiros:

$$P(x) = \sum_{k=0}^{m} a_k x^k .$$

Por ser $10 \equiv -1$ (mod.11), temos (Lema 20.1):

$$P(10) \equiv P(-1) \pmod{11}$$

Como $P(10) = n$ e $P(-1) = T$, segue-se que $n \equiv T \pmod{11}$. Portanto, $n \equiv 0 \pmod{11}$ se e somente se $T \equiv 0 \pmod{11}$, isto é, $11|n$ se e somente se $11|T$.

Assim, p.ex., o inteiro $n = 1571724$ é *divisível por* 11, porque a soma alternada:

$$T = 4 - 2 + 7 - 1 + 7 - 5 + 1 = 11$$

é divisível por 11.

Note-se que este inteiro também é *divisível por* 9, porque a soma dos seus algarismos é 27 e 27 é divisível por 9.

EXERCÍCIOS

1. Escrever $(31322)_4$ e $(5a19)_{11}$ no sistema de *base* 10.

2. Escrever no sistema de *base* 10:

$$(3141)_5, \quad (3141)_7 \quad \text{e} \quad (3141)_{11}.$$

3. Escrever 132 e 285 no sistema de *base* 8.

4. Escrever 1492 nos sistemas de *base* 2, 3, 7, 9 e 11.

5. Escrever $(7645)_8$ no sistema de *base* 5 e $(a3b)_{12}$ no sistema de *base* 7.

6. Resolver as seguintes equações:

$(123)_4 = x_5$, $(234)_5 = x_6$, $(123)_x = (1002)_4$

7. Escrever 2417 no sistema de *base* 5 e 1639 no sistema de *base* 7.

8. Determinar a *base* do sistema no qual 73 se escreve 243.

9. Determinar a *base* do sistema no qual $(346)_7$ se escreve 91.

10. Escrever $(3ab7)_{12}$ no sistema de *base* 10.

11. Construir as *tábuas* de adição e de multiplicação no sistema de *base*2.

12. Usando o *critério de divisibilidade por* 9, determinar se os inteiros 374518 e 1520397 são divisíveis por 9.

13. Usando o *critério de divisibilidade por* 11, determinar se os inteiros 370546 e 22481907 são divisíveis por 11.

14. Usando os *critérios de divisibilidade por* 9 *e por* 11, determinar se os inteiros 176521221 e 149235678 são divisíveis por 9 ou 11.

15. Demonstrar que um inteiro é *divisível por* 3 se e somente se a soma dos seus algarismos é divisível por 3.

16. Demonstrar que um inteiro é *divisível por* 4 se e somente se o número formado pelo seu algarismo das dezenas e pelo seu algarismo das unidades é divisível por 4.

17. Determinar o algarismo x de modo que o inteiro:

(a) 5x9 seja divisível por 9

(b) 45x3x seja divisível por 3

(c) 7x6 seja divisível por 3 e por 4

(d) 934x1x seja divisível por 2 e por 3

(e) 50x2x seja divisível por 2, por 3 e por 11

18. Demonstrar que um inteiro é *divisível por* 8 se e somente se o número formado pelos seus três últimos algarismos da direita é *divisível por* 8.

19. Determinar os algarismos x e y de modo que o inteiro:

(a) 67xy seja divisível por 5 e por 11

(b) 5x6y seja divisível por 3 e por 4

(c) 56x21y seja divisível por 9 e por 10

(d) 34xx58y seja divisível por 9 e por 11

(e) 231xy seja divisível por 5 e por 9

(f) 514xy seja divisível por 8 e por 9

20. Mostrar que a diferença entre os inteiros abc e cba ($a > c$) é um múltiplo de 11.

21. Mostrar que todo inteiro com três algarismos, todos iguais, é *divisível por* 37.

22. Escreve-se, à esquerda de um inteiro com dois algarismos, o dobro desse inteiro. Mostrar que o novo inteiro que assim se obtém é *divisível por* 67.

23. Demonstrar que um inteiro é *divisível por* 4 se e somente se a soma do algarismo das unidades com o dobro do algarismo das dezenas é *divisível por* 4.

24. Determinar os algarismos x e y de modo que o inteiro:
    (a) x0y seja divisível por 12
    (b) 5x2y seja divisível por 15
    (c) 28x75y seja divisível por 33
    (d) 1234xy seja divisível por 72
    (e) 3262xy seja divisível por 36
    (f) 7x36y5 seja divisível por 1375

25. Mostrar que todo inteiro formado de seis algarismos, todos iguais, é divisível por 7, 11, 13 e 37.

26. Mostrar que a soma dos seis inteiros de dois algarismos que se podem formar com três algarismos diferentes é igual a 22 vezes a soma desses algarismos.

27. Demonstrar que um inteiro é *divisível por* 8 se e somente se a soma do algarismo das unidades, mais o dobro do algarismo das dezenas, mais o quádruplo do algarismo das centenas é *divisível por* 8.

28. Demonstrar que um inteiro é *divisível por* 6 se e somente se a soma do algarismo das unidades com o quádruplo da soma de todos os outros algarismos é *divisível por* 6.

29. Demonstrar que, para todo inteiro a, o algarismo das unidades de a^4 é 0, 1, 5 ou 6.

30. Demonstrar que o algarismo das unidades de um *número triangular* é 0,1,3,5,6 ou 8.

31. O inteiro xy243z é divisível por 396. Determinar os algarismos x, y e z do dividendo.

CAPÍTULO 21

RAÍZES PRIMITIVAS

21.1 ORDEM DE UM INTEIRO MÓDULO N

Sejam a e $n > 1$ inteiros tais que o mdc(a,n) = 1. Pelo *teorema de EULER:*

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

mas podem haver potências de a menores que $a^{\phi(n)}$ e que são congruentes a 1 módulo n. Assim, p.ex.:

$$3^3 \equiv 1 \pmod{13}, \quad 3^6 \equiv 1 \pmod{13} \quad \text{e} \quad 3^3 < 3^6 < 3^{\phi(13)}$$

Definição 21.1 Sejam a e $n > 1$ inteiros tais que o mdc(a,n) = 1. Chama-se *ordem de a módulo n* o menor inteiro positivo k tal que

$$a^k \equiv 1 \pmod{n}$$

Indica-se que a *ordem de* $\underline{a}$ *módulo* $\underline{n}$ *é* $\underline{k}$ com a notação:

$$o_n(a) = k.$$

Assim, p.ex., com $a = 2$ e $n = 7$, temos:

$$2^1 \equiv 2 \pmod{7}, \quad 2^2 \equiv 4 \pmod{7}, \quad 2^3 \equiv 1 \pmod{7}$$

$$2^4 \equiv 2 \pmod{7}, \quad 2^5 \equiv 4 \pmod{7}, \quad 2^6 \equiv 1 \pmod{7}, \ldots$$

Portanto, o inteiro 2 tem *ordem* 3 *módulo* 7, isto é:

$$o_7(2) = 3.$$

NOTA. Não existe inteiro positivo $\underline{k}$ tal que

$$a^k \equiv 1 \pmod{n} \quad \text{se o} \quad mdc(a,n) > 1$$

porque, se existisse, então $x = a^{k-1}$ seria uma *solução* da congruência linear $ax \equiv 1 \pmod{n}$, o que é *impossível* (Teorema 10.1).

Cumpre ainda observar que, se dois inteiros $\underline{a}$ e $\underline{b}$ são congruentes módulo $\underline{n}$, então $\underline{a}$ e $\underline{b}$ *tem a mesma ordem módulo* $\underline{n}$, porque

$$a \equiv b \pmod{n} \quad \text{e} \quad a^k \equiv 1 \pmod{n}$$

implica:

$$a^k \equiv b^k \equiv 1 \pmod{n}$$

<u>Exemplo 21.1</u> Achar as *ordens módulo* 11 dos inteiros positivos menores que 11.

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}
1	1	1	1	1	1	1	1	1	1
2	4	8	5	10	9	7	3	6	1
3	9	5	4	1	3	9	5	4	1
4	5	9	3	1	4	5	9	3	1
5	3	4	9	1	5	3	4	9	1
6	3	7	9	10	5	8	4	2	1
7	5	2	3	10	4	6	9	8	1
8	9	6	4	10	3	2	5	7	1
9	4	3	5	1	9	4	3	5	1
10	1	10	1	10	1	10	1	10	1

Consoante a tabela acima, temos:

$$o_{11}(1) = 1, \quad o_{11}(2) = o_{11}(6) = o_{11}(7) = o_{11}(8) = 10$$

$$o_{11}(3) = o_{11}(4) = o_{11}(5) = o_{11}(9) = 5, \; o_{11}(10) = 2.$$

Observe-se que as *ordens* 1, 2, 5 e 10 são *divisores* de $\phi(11) = 10$.

<u>Teorema 21.1</u> Seja <u>a</u> um inteiro que tem *ordem k módulo* <u>*n*</u>. Então:

$$a^h \equiv 1 \pmod{n}$$

se e somente se <u>k</u> divide <u>h</u> $(k|h)$.

Demonstração:

($\Longrightarrow$) Suponhamos que $k|h$, isto é, $h = kq$, onde $\underline{q}$ é um inteiro. Por ser $o_n(a) = k$, temos:

$$a^k \equiv 1 \pmod{n} \Longrightarrow (a^k)^q = a^h \equiv 1 \pmod{n}$$

($\Longleftarrow$) Reciprocamente, suponhamos que $a^h \equiv 1 \pmod{n}$, sendo $\underline{h}$ um inteiro positivo. Pelo algoritmo da divisão, temos:

$$h = kq + r, \quad \text{com} \quad 0 \leqslant r < k$$

Portanto:

$$a^h = a^{kq+r} = (a^k)^q a^r$$

Mas, por hipótese: $a^h \equiv 1 \pmod{n}$ e $a^k \equiv 1 \pmod{n}$, o que implica:

$$a^r \equiv 1 \pmod{n}$$

Como $\underline{k}$ é o *menor* inteiro positivo tal que $a^k \equiv 1 \pmod{n}$ e $0 \leqslant r < k$, segue-se que $r = 0$. Logo, $h = kq$ e $k|h$.

Corolário 21.1 Se o inteiro $\underline{a}$ tem *ordem* $\underline{k}$ *módulo* $\underline{n}$, então $k|\phi(n)$.

Demonstração:

Pelo *teorema de EULER:* $a^{\phi(n)} \equiv 1 \pmod{n}$. Logo, pelo teorema 20.1: $k \mid \phi(n)$.

Assim, p.ex., a *ordem* de um inteiro módulo 9 só pode ser um *divisor* de $\phi(9) = 6$, isto é, 1, 2, 3 ou 6.

Exemplo 21.2 Determinar a *ordem de* 2 *módulo* 13.

Por ser $\phi(13) = 12$, a ordem de 2 módulo 13 é um dos *divisores* de 12, isto é, 1, 2, 3, 4, 6, 12. Temos:

$$2^1 \equiv 2, \quad 2^2 \equiv 4, \quad 2^3 \equiv 8 \pmod{13}$$

$$2^4 \equiv 3, \quad 2^6 \equiv 12, \quad 2^{12} \equiv 1 \pmod{13}$$

Portanto, 2 tem *ordem* 12 *módulo* 13.

Teorema 21.2 Se a *ordem* do inteiro a *módulo* n é k, então:

$$a^i \equiv a^j \pmod{n}$$

se e somente se $i \equiv j \pmod{k}$.

Demonstração:

($\Longrightarrow$) Suponhamos que $a^i \equiv a^j \pmod{n}$, onde $i \geq j$. Como o $mdc(a,n) = 1$, podemos *cancelar* o fator comum a^j, o que dá:

$$a^{i-j} \equiv 1 \pmod{n}$$

Logo, pelo teorema 20.1, $k|(i-j)$ e isto significa que $i \equiv j \pmod{k}$.

($\Longleftarrow$) Reciprocamente, suponhamos que $i \equiv j \pmod{k}$. Então, $i = j + kq$, onde $\underline{q}$ é um inteiro, e como $a^k \equiv 1 \pmod{n}$, temos:

$$a^i \equiv a^{j+kq} \equiv a^j(a^k)^q \equiv a^j \pmod{n}$$

<u>Corolário 21.2</u> Se $\underline{a}$ tem *ordem* $\underline{k}$ *módulo* $\underline{n}$, então os inteiros:

$$a, a^2, \ldots, a^k$$

são *incongruentes módulo* $\underline{n}$.

<u>Demonstração:</u>

Com efeito, se $a^i \equiv a^j \pmod{n}$ para $1 \leqslant i \leqslant j \leqslant k$, então, pelo teorema anterior, $i \equiv j \pmod{k}$. Mas isto somente é possível se $i = j$.

<u>Teorema 21.3</u> Se o inteiro $\underline{a}$ tem *ordem* $\underline{k}$ *módulo* $\underline{n}$ e $h > 0$, então a^h tem *ordem* $k/\text{mdc}(h,k)$ *módulo* $\underline{n}$.

Demonstração:

Seja $d = mdc(h,k)$, de modo que $h = dh_1$ e $k = dk_1$, com o $mdc(h_1,k_1) = 1$.

Obviamente:

$$(a^h)^{k_1} = (a^{dh_1})^{k/d} = (a^k)^{h_1} \equiv 1 \ (mod.n)$$

Posto isto, suponhamos que a^h tem *ordem* $\underline{r}$ *módulo* $\underline{n}$. Então, $r|k_1$ (Teorema 20.1), e como $\underline{a}$ tem *ordem* $\underline{k}$ *módulo* $\underline{n}$, a congruência:

$$a^{hr} \equiv (a^h)^r \equiv 1 \ (mod.n)$$

mostra que $k|hr$ (Teorema 20.1) e, portanto:

$$dk_1|dh_1r \quad ou \quad k_1|h_1r.$$

Mas, o $mdc(h_1,k_1) = 1$, de modo que $k_1|r$. Assim sendo, $r|k_1$ e $k_1|r$, o que implica:

$$r = k_1 = k/d = k/mdc(h,k)$$

Corolário 21.3 Seja $\underline{a}$ um inteiro que tem *ordem* $\underline{k}$ *módulo* $\underline{n}$. Então, a^h tem *ordem* $\underline{k}$ *módulo* $\underline{n}$ se e somente se o $mdc(h,k) = 1$.

Demonstração:

Com efeito, se o $mdc(h,k) = 1$, então a^h tem ordem $k/1 = k$

módulo $\underline{n}$ (Teorema 20.3).

Reciprocamente, se a^h tem *ordem* $\underline{k}$ *módulo* $\underline{n}$ e o mdc(h,k) = = d, então:

$$1 \equiv a^k \equiv (a^k)^{h/d} \equiv (a^h)^{k/d} \pmod{n}$$

Portanto, $\underline{k}$ divide k/d (Teorema 20.1), o que implica d = mdc(h,k) = 1.

Exemplo 21.3 A tabela abaixo dá as *ordens módulo* 13 dos inteiros positivos menores que 13.

a	1	2	3	4	5	6	7	8	9	10	11	12
$o_{13}(a)$	1	12	3	6	4	12	12	4	3	6	12	2

Observe-se que a *ordem de* 2 *módulo* 13 é 12 e que as *ordens* de $2^2 = 4$ e $2^3 = 8$ são 6 e 4, respectivamente, tais que

$$6 = 12/\text{mdc}(2,12) \quad \text{e} \quad 4 = 12/\text{mdc}(3,12)$$

conforme ensina o Teorema 20.3.

Os inteiros que também têm *ordem* 12 *módulo* 13 são potências 2^k tais que o mdc(k,12) = 1, isto é:

$$2^5 \equiv 6, \quad 2^7 \equiv 11, \quad 2^{11} \equiv 7 \pmod{13}.$$

Note-se ainda que os inteiros:

$$2,\ 2^2,\ 2^3,\ \ldots,\ 2^{12}$$

são *incongruentes módulo* 13 (Corolário 20.2).

21.2 RAIZ PRIMITIVA DE UM INTEIRO

Definição 21.2 Chama-se *raiz primitiva* de um inteiro positivo n um inteiro a tal que o mdc(a,n) = 1 e a *ordem de* a *módulo* n é $\phi(n)$.

Em outros termos, *raiz primitiva* de um inteiro positivo n é um inteiro a tal que

$$a^{\phi(n)} \equiv 1 \pmod{n} \quad \text{e} \quad a^k \not\equiv 1 \pmod{n}$$

para todo inteiro positivo $k < \phi(n)$.

Assim, p.ex. 3 é uma *raiz primitiva* de 7, porque o mdc(3,7) = 1 e a *ordem de* 3 *módulo* 7 é $\phi(7) = 6$, pois, temos:

$$3^1 \equiv 3,\quad 3^2 \equiv 2,\ 3^3 \equiv 6,\ 3^4 \equiv 4,\ 3^5 \equiv 5,\ 3^6 \equiv 1 \pmod{7}$$

Para os inteiros positivos *compostos* nem sempre existem *raízes primitivas*, sendo a existência mais uma exceção do que uma regra, mas todo *primo* p tem precisamente $\phi(p-1)$ *raízes primitivas*.

Exemplo 21.4 O inteiro 2 é uma *raiz primitiva* de 9 *(composto)*, pois, temos:

$$2^{\phi(9)} = 2^6 \equiv 1 \pmod{9} \quad \text{e} \quad 2^k \not\equiv 1 \pmod{9}$$

para $k = 1,2,3,4,5$.

Teorema 21.4 Sejam a e $n > 1$ inteiros tais que o $mdc(a,n) = 1$, e sejam

$$a_1, a_2, \ldots, a_{\phi(n)}$$

os inteiros positivos *menores que* n e que são *primos com* n. Se a é uma *raiz primitiva* de n, então as potências:

$$a, a^2, \ldots, a^{\phi(n)}$$

são *congruentes módulo* n aos inteiros

$$a_1, a_2, \ldots, a_{\phi(n)},$$

não necessariamente nesta ordem.

Demonstração:

Como a e n são *primos entre si*, o mesmo ocorre com toda potência de a e n. Portanto, cada a^k é congruente módulo n a algum dos a_i. E como as $\phi(n)$ potências de a: $a, a^2, \ldots, a^{\phi(n)}$ são *incongruentes módulo* n (Corolário 21.2), segue-se que estas $\phi(n)$ potências de a são *congruentes módulo* n aos $\phi(n)$ inteiros $a_1, a_2, \ldots, a_{\phi(n)}$,

não necessariamente nesta ordem.

Assim, p.ex., 2 é uma *raiz primitiva* de 9, e as potências de 2:

$$2,\ 2^2,\ 2^3,\ 2^4,\ 2^5,\ 2^6$$

são *congruentes módulo* 9 aos inteiros *menores que* 9 *e primos com* 9:

$$2,\ 4,\ 8,\ 7,\ 5,\ 1$$

<u>Corolário 21.4</u> Se <u>n</u> tem uma *raiz primitiva*, então <u>n</u> tem precisamente $\phi(\phi(n))$ *raizes primitivas*.

<u>Demonstração:</u>

Suponhamos que <u>a</u> é uma *raiz primitiva* de <u>n</u>. Pelo teorema anterior, qualquer outra *raiz primitiva* de <u>n</u> se encontra entre os elementos do conjunto:

$$\left\{ a,\ a^2,\ \ldots,\ a^{\phi(n)} \right\}.$$

Mas, o número de potências a^k, onde $1 \leqslant k \leqslant \phi(n)$, que têm *ordem* $\phi(n)$, é igual ao número de inteiros <u>k</u> tais que o $\text{mdc}(k, \phi(n)) = 1$, e como o número de tais inteiros é $\phi(\phi(n))$, segue-se que <u>n</u> tem exatamente $\phi(\phi(n))$ *raizes primitivas*.

Assim, p.ex., 2 é uma *raiz primitiva* de 11 e, portanto 11 tem exatamente

$$\phi(\phi(11) = \phi(10) = 4$$

raizes primitivas, que são os inteiros 2, 6, 7 e 8.

NOTA. Um inteiro $n > 1$ tem uma *raiz primitiva* se e somente se

$$n = 2,\ 4,\ p^k,\ 2p^k$$

onde $\underline{p}$ é um *primo ímpar* e $k \geqslant 1$.

EXERCÍCIOS

1. Achar as *ordens* dos inteiros 2, 3 e 5: (a) módulo 17; (b) módulo 19; (c) módulo 23.

2. Achar as *ordens* dos inteiros 2,4,7,8,11,13 e 14(mod.15).

3. Achar os inteiros que tem *ordem* 6 (mod.31).

4. Demonstrar as seguintes proposições:

   (a) Se $\underline{a}$ tem *ordem* hk (mod.n), então a^h tem *ordem* $\underline{k}$ (mod.n).

(b) Se a tem *ordem* 2k módulo o *primo ímpar* p, então $a^k \equiv -1$ (mod.p).

(c) Se a tem *ordem* n-1 (mod.n), então n é um *primo*.

5. As *ordens* respectivas de a e b módulo n são h e k. Mostrar que a *ordem* de ab (mod.n) divide hk. Em particular, se o mdc(h,k) = 1, então a *ordem* de ab (mod.n) é hk.

6. Mostrar que, se a tem *ordem* 3 (mod.p), então a+1 tem *ordem* 6 (mod.p).

7. Mostrar que 2 é uma *raiz primitiva* de 19, mas não de 17.

8. Mostrar que 15 não tem *raízes primitivas* calculando as *ordens* dos inteiros 2,4,7,8,11,13 e 14 (mod.15).

9. Achar duas *raizes primitivas* de 10.

10. Sabendo que 3 é uma *raiz primitiva* de 17, achar todas as outras *raizes primitivas* de 17.

11. Sabendo que 2 é uma *raiz primitiva* de 19, achar todas as outras *raizes primitivas* de 19.

12. Achar todas as *raizes primitivas* de 5, 9, 11 e 13.

EXERCÍCIOS SUPLEMENTARES

1. Demonstrar que, se $\underline{a}$ e $\underline{b}$ são inteiros, com $b > 0$, então *existem* e são *únicos* os inteiros $\underline{q}$ e $\underline{r}$ tais que $a = bq + r$, onde $2b \leqslant r < 3b$.

2. Verificar que, se um inteiro $\underline{n}$ é ao mesmo tempo um *quadrado perfeito* e um *cubo perfeito* (como $64 = 8^2 = 4^3$), então $\underline{n}$ é da forma $7k$ ou $7k+1$.

3. Demonstrar que, se $\underline{a}$ e $\underline{b}$ são inteiros, com $b \neq 0$, então *existem* e são *únicos* os inteiros $\underline{q}$ e $\underline{r}$ tais que $a = bq + r$, onde $-|b|/2 < r \leqslant |b|/2$.

4. Demonstrar que nenhum inteiro da sequência:

$$11,\ 111,\ 1111,\ 11111,\ \ldots$$

é um *quadrado perfeito*.

5. Demonstrar que $4 \nmid (a^2 + 2)$, qualquer que seja o inteiro $\underline{a}$.

6. Demonstrar que 3 divide $2^n + (-1)^{n+1}$, onde $n \geqslant 1$.

7. Demonstrar que, se $\underline{a}$ é um inteiro tal que $2 \nmid a$ e $3 \nmid a$, então 24 divide $a^2 - 1$.

8. Demonstrar que a soma dos quadrados de dois inteiros ímpares não pode ser um *quadrado perfeito*.

9. Demonstrar que o produto de três inteiros consecutivos é divisível por 6 e que o produto de quatro inteiros consecutivos é divisível por 24.

10. Demonstrar que $360 | a^2(a^2 - 1)(a^2 - 4)$, qualquer que seja o inteiro $\underline{a}$.

11. Demonstrar que o produto de cinco inteiros consecutivos é divisível por 120.

12. Sejam $\underline{a}$ e $\underline{b}$ inteiros *não nulos*. Demonstrar:

    (a) Se $k > 0$, então o $\text{mmc}(ka, kb) = k.\text{mmc}(a,b)$.

    (b) Se $\underline{m}$ é um múltiplo comum de $\underline{a}$ e $\underline{b}$, então o $\text{mmc}(a,b) | m$.

13. Sejam $\underline{p}$ e $\underline{p+2}$ *primos gêmeos*. Demonstrar que $p(p+2)+1$ é um *quadrado perfeito* e que $p+(p+2)$, com $p > 3$, é *divisível por* 12.

14. Mostrar que, se $n > 3$, os inteiros n, $n+2$ e $n+4$ não podem ser todos *primos*.

15. Demonstrar que, se o conjunto $\{a_1, a_2, \ldots, a_n\}$ é um *sistema completo de restos módulo* $\underline{n}$ e se o $\text{mdc}(a,n) = 1$, então o conjunto $\{aa_1, aa_2, \ldots, aa_n\}$ também é um *sistema completo de restos módulo* $\underline{n}$.

16. Verificar que o conjunto $\{0,1,2,2^2,2^3,\ldots,2^9\}$ é um *sistema completo de restos módulo* 11, mas que o conjunto $\{0,1^2, 2^2, 3^2, \ldots, 10^2\}$ não o é.

17. Demonstrar as seguintes proposições:

(a) Se o $mdc(a,n) = 1$, então o conjunto de inteiros:

$$\{c, c+a, c+2a, \ldots, c+(n-1)a\}$$

é um *sistema completo de restos módulo* $\underline{n}$, qualquer que seja $\underline{c}$.

(b) Todo conjunto de $\underline{n}$ inteiros consecutivos é um *sistema completo de restos módulo* $\underline{n}$.

18. Verificar que, se $a \equiv b \pmod{m_1}$ e se $a \equiv b \pmod{m_2}$, então:

$$a \equiv b \pmod{m}, \text{ onde } m = mmc(m_1,m_2)$$

Em particular, se m_1 e m_2 são *primos entre si*, então $a \equiv b \pmod{m_1 m_2}$.

19. Demonstrar que, se $ab \equiv cd \pmod{m}$ e se $b \equiv d \pmod{m}$, com o $mdc(b,n) = 1$, então $a \equiv c \pmod{m}$.

20. Demonstrar que, se $a \equiv b \pmod{m_1}$ e se $a \equiv c \pmod{m_2}$, então:

$$b \equiv c \pmod{m}, \text{ onde } m = mdc(m_1,m_2)$$

21. Achar os dois últimos algarismos do inteiro 9^{9^9}.

22. Usando os *critérios de divisibilidade por* 9 ou *por* 11, determinar os algarismos x e y nas duas seguintes igualdades:

(a) $2x99561 = \left[3(523 + x)\right]^2$

(b) $52817 \times 3212146 = 169655y15282$

23. Achar o menor inteiro $a > 2$ tal que $2|a$, $3|(a+1)$, $4|(a+2)$, $5|(a+3)$ e $6|(a+4)$.

24. Determinar o menor inteiro positivo que deixa os *restos:*

(a) 1,2,55 quando dividido por 2,3,6,12, respectivamente;

(b) 2,3,4,5 quando dividido por 3,4,5,6, respectivamente;

(c) 3,11,15 quando dividido por 10,13,17,respectivamente;

25. Mostrar que, se o $mdc(a,42) = 1$, então $168 = 3.7.8$ divide $a^6 - 1$.

26. Mostrar que, se o $mdc(a,133) = mdc(b,133) = 1$, então $133|(a^{18} - b^{18})$.

27. Mostrar que a^5 e a têm o mesmo algarismo das unidades, qualquer que seja o inteiro a.

28. Demonstrar que $a^{13} \equiv a \pmod{3.7.13}$, qualquer que seja o inteiro $\underline{a}$.

29. Usando o *teorema de FERMAT*, achar o algarismo das unidades de 3^{100}.

30. Demonstrar que $d(n)$ é um inteiro ímpar se e somente se $\underline{n}$ é um *quadrado perfeito*.

31. Demonstrar:

$$\sum_{d|n} 1/d = s(n)/n$$

32. Verificar que $s(n+2) = s(n)+2$ para $n = 434$ e $n=8575$.

33. Demonstrar que, se $\underline{n}$ e $n+2$ são *primos gêmeos*, então:

$$s(n+2) = s(n)+2$$

34. Demonstrar que $s(n)$ é um inteiro ímpar se e somente se $\underline{n}$ é um quadrado perfeito ou o dobro de um quadrado perfeito.

35. Demonstrar que, se $n > 1$ é um inteiro *composto*, então $s(n) > n + \sqrt{n}$.

36. Sejam $\underline{m}$ e $\underline{n}$ inteiros positivos. Demonstrar:

(a) $\phi(m)\phi(n) = \phi(mn)\phi(d)/d$, onde $d = mdc(m,n)$

(b) $\phi(m)\phi(n) = \phi(mdc(m,n))\phi(mmc(m,n))$

37. Mostrar que a equação $\phi(n) = 14$ não tem solução.

38. Usando o *teorema de EULER*, demonstrar:

(a) $a^{37} \equiv a \pmod{1729 = 7.13.19}$, qualquer que seja o inteiro $\underline{a}$.

(b) $a^{13} \equiv a \pmod{2730 = 2.3.5.7.13}$, qualquer que seja o inteiro $\underline{a}$.

(c) $a^{33} \equiv a \pmod{4080 = 15.16.17}$, qualquer que seja o inteiro ímpar $\underline{a}$.

39. Sejam $\underline{m}$ e $\underline{n}$ inteiros positivos *primos entre si*. Demonstrar:

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$$

40. Achar o menor inteiro ímpar $n > 3$ tal que $3|n$, $5|(n+2)$ e $7|(n+4)$.

41. Achar o algarismo das unidades de 7^{355}.

42. Achar o *resto* quando 314^{162} é dividido por 163.

43. Seja $f(n) = (n + \phi(n))/2$. Mostrar que $f(f(n)) = \phi(n)$ se $n = 2^k$, onde $k = 2,3,\ldots$

44. Achar todas as soluções da equação $\phi(n) = 4$.

45. Mostrar que pq $(pq \neq 6)$ é *deficiente*.

46. Mostrar que p^k, $k \geqslant 1$, é *deficiente*.

47. Achar os valores de $\underline{k}$ para os quais $2^k.11$ é *abundante*.

48. Mostrar que, se o mdc(a,b) = 1 e se $\underline{a}$ é *abundante*, então $\underline{ab}$ é *abundante*.

49. Mostrar que, se $6|n$, então $\phi(n) \leqslant n/3$.

50. Achar o menor *primo* para o qual 10 é uma *raiz primitiva*.

51. Mostrar que 2 não é uma *raiz primitiva* de 31.

52. Mostrar que o quadrado de qualquer múltiplo ímpar de 3 é a diferença de dois *números triangulares*, isto é:

$$9(2n+1)^2 = t_{9n+4} - t_{3n+1}$$

53. Mostrar que, se $2n^2 \pm 1$ é um quadrado perfeito:

$$2n^2 \pm 1 = m^2,$$

então $(mn)^2$ é um *número triangular*. Dar três exemplos de quadrados perfeitos que também são *números triangulares*.

54. Achar um divisor *primo* do inteiro $n = 4(3.7.11) - 1$ da forma $4k+3$.

55. Achar a *forma* de todos os inteiros positivos $\underline{n}$ tais que $d(n) = 10$ e o menor inteiro positivo que verifica esta igualdade.

56. Resolver as seguintes equações:

(a) $\phi(n) = 16$

(b) $\phi(n) = 24$

(c) $\phi(n) = 30$

57. Demonstrar que a equação $\phi(n) = 2p$ não tem solução quando $\underline{p}$ é um *primo* e $2p+1$ é *composto*.

58. Chama-se *sistema reduzido de restos módulo* $\underline{m}$ todo conjunto de $\phi(m)$ inteiros, incongruentes módulo $\underline{m}$, cada um dos quais é primo com $\underline{m}$. Verificar:

(a) o conjunto de inteiros $\{-31,-16,-8,13,25,80\}$ é um sistema reduzido de restos módulo 9;

(b) o conjunto de inteiros $\{3,3^2,3^3,3^4,3^5,3^6\}$ é um sistema reduzido de restos módulo 14;

(c) o conjunto de inteiros $\{2,2^2,2^3,\ldots,2^{18}\}$ é um sistema reduzido de restos módulo 27.

59. Determinar quais dos seguintes conjuntos são sistemas reduzidos de restos módulo 5:

(a) $\{0,1,2,3,4\}$ (b) $\{1,-2,3,-4\}$

(c) $\{16,9,-2,7\}$ (d) $\{6,11,16,21\}$

60. Seja $\underline{p}$ um primo ímpar. Mostrar que o conjunto:

$$\{-(p-1)/2,\ldots,-2,-1,1,2,\ldots,(p-1)/2\}$$

é um sistema reduzido de restos módulo $\underline{p}$.

61. Demonstrar que, se S é um sistema reduzido de restos módulo m e se o mdc(a,m) = 1, então o conjunto $T = \{ ax \mid x \in S \}$ também é um sistema reduzido de restos módulo m.

62. Resolver a equação: $u(n) + u(n+1) + u(n+2) = 3$, sendo u a função de MOBIUS.

63. Mostrar que um *número triangular* não pode terminar em 2,4,7 ou 9.

64. Um inteiro composto n tal que $n \mid (2^n - 2)$ chama-se *pseudo-primo*. Verificar que 341, 561, 645 e 1105 são *pseudo-primos*.

65. Mostrar que, se $2^{k+1} - 1$ é *composto*, então o inteiro $n = 2^k(2^{k+1} - 1)$ é *abundante*.

66. Mostrar que $\phi(n) = n/3$ se e somente se $n = 2^k 3^j$, onde k e j são inteiros positivos.

67. Calcular $\sum_{d \mid n} (-1)^{n/d} \phi(d)$ para os seguintes valores de n:

(a) n = 12, 13, 14, 15, 16.
(b) n = p, sendo p um primo ímpar.
(c) $n = 2^k$, sendo $k \geqslant 1$.
(d) $n = p^k$, sendo $k \geqslant 1$ e p um primo ímpar.

68. Mostrar que, se $a+b$ é *par*, então $24 | ab(a^2 - b^2)$.

69. Demonstrar que, se $210m + n$ é *primo*, onde $0 \leq n < 121$, entao $\underline{n}$ é *primo*.

70. Mostrar que todo *divisor proprio* de um número perfeito par é um *número deficiente*.

71. Mostrar que, se $n = (6m+1)(12m + 1)(18m+1)$, então $n-1$ é divisível por $36m$.

72. Demonstrar que a soma $2p+2$ de *primos gêmeos* $\underline{p}$ e $\underline{p+2}$, onde $p > 3$, é divisível por 12.

73. Seja $\underline{p}$ um primo ímpar. Determinar o número de elementos em cada uma das sequências:

$$1.2,\ 2.3,\ 3.4, \ldots,\ p(p+1)$$

$$1.2,\ 2.3,\ 3.4, \ldots,\ p^2(p^2+1)$$

que são primos com $\underline{p}$.

74. Mostrar que a *média harmônica* dos divisores de um número perfeito par é um inteiro.

75. Mostrar que $2n^2 - 3$ nunca é um *quadrado perfeito*, onde $n = 2,3,4,\ldots$.

76. Demonstrar por *indução matemática* que

$$3^{n+2} | 10^{3n} - 1, \quad n = 0,1,2, \ldots$$

77. Seja $\underline{n}$ um número perfeito par. Demonstrar que $\prod_{d|n} d$ é uma potência de $\underline{n}$.

78. Mostrar que a sequência 5,12,19,26,... não contém termo algum da forma 2^n ou $2^n - 1$.

79. Mostrar que o inteiro 111...11 com $\underline{n}$ algarismos 1 é composto se $\underline{n}$ é composto.

80. Mostrar que, se $\underline{n}$ é a soma de dois *números triangulares*, então $4n+1$ é uma soma de dois quadrados.

81. Mostrar que $a^5 \equiv a \pmod{10}$, qualquer que seja o inteiro $\underline{a}$.

82. Demonstrar que todo inteiro compreendido entre dois *primos gêmeos*, exceto, 3,5 e 5,7, é *abundante*.

83. Sejam $\underline{m}$ e $\underline{n}$ *números amigos*. Demonstrar:

$$\left(\sum_{d|m} 1/d\right)^{-1} + \left(\sum_{d|n} 1/d\right)^{-1} = 1$$

84. Um inteiro diz-se *sem quadrados* se não é divisível pelo quadrado de qualquer inteiro maior que 1. Demonstrar:

(a) um inteiro $n > 1$ é *sem quadrados* se e somente se $\underline{n}$ é um produto de *primos distintos*, isto é: $n = p_1 p_2 \cdots p_k$, onde os p_i são *primos* todos *distintos*;

(b) todo inteiro $n > 1$ é o produto de um quadrado perfeito por um *sem quadrados*, isto é: $n = a^2 b$, onde b é *sem quadrados*.

85. Demonstrar que o cubo de qualquer inteiro pode ser expresso como a diferença de dois quadrados.

86. Seja m um inteiro qualquer e seja n o inteiro que se obtém invertendo a *ordem* dos algarismos de m (p.ex., se $m = 7925$, então $n = 5297$). Mostrar que a diferença $m - n$ é divisível por 9.

87. Mostrar que os inteiros:

$$1111,\ 111111,\ 11111111,\ \ldots,\ 111\ldots11,\ \ldots$$

cada um dos quais é formado por um número *par* de algarismos 1, são todos *compostos*.

88. Calcular a soma: $1 + 11 + 111 + \ldots + 111\ldots1$, onde a última parcela é formada de n algarismos 1.

89. Demonstrar que o produto $P = (n+1)(n+2)\ldots 2n$ de n inteiros consecutivos é divisível pelo produto $P_1 = 1.3.5\ldots(2n-1)$ dos n primeiros inteiros ímpares e achar o quociente.

90. Um inteiro positivo dividido por 5 dá resto 3 e dividido por 9 dá resto 4. Determinar o resto da divisão desse inteiro por $45 = 5 \times 9$.

91. Calcular o *resto* da divisão por 8 de $4365^{43} \times 7937^{67}$.

92. Mostrar que são *falsas* as proposições (a) e (b), dando um *contra-exemplo* para cada uma delas:

    (a) Se $a^2 | b^3$, então $a | b$

    (b) Se $b | (a^2+1)$, então $b | (a^4+1)$.

93. Demonstrar que, se o $mdc(a,b) = 1$, então o $mdc(a \pm b, ab) = 1$.

94. Achar as soluções inteiras e positivas da equação $x^2 - y^2 = 499$.

95. Determinar o inteiro $n = 2^x.3^y.5^z$, sabendo que dividido por 12, por 18 e por 90 perde, respectivamente, 24, 27 e 30 dos seus divisores.

96. Achar os inteiros de três algarismos divisíveis ao mesmo tempor 14 e 34.

97. Sabendo que o $mdc(n,54) = mdc(n,126) = 6$, calcular o inteiro n.

98. Sabendo que o $mmc(35,n) = 180$ e que o $mmc(84,n)=1260$, calcular o inteiro n.

99. Determinar o número de inteiros compreendidos entre 100 e 1000 que são divisíveis por 7.

100. Sejam $\underline{p}$ e $\underline{q}$ primos distintos. Demonstrar:

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$$

101. Mostrar que os inteiros $1729 = 7.13.19$ e $1905 = 3.5.127$ são ambos *pseudo-primos*.

102. Seja $\underline{n}$ um inteiro *sem quadrados*. Demonstrar que $d(n) = 2^r$, onde $\underline{r}$ é o número de divisores primos de $\underline{n}$.

103. Determinar quais dos seguintes conjuntos são *sistemas completos de restos módulo* 11:

(a) $\{0,1,2,4,8,16,32,64,128,256,512\}$

(b) $\{1,3,5,7,9,11,13,15,17,19,21\}$

(c) $\{2,4,6,8,10,12,14,16,18,20,22\}$

(d) $\{-5,-4,-3,-2,-1,0,1,2,3,4,5,\}$

104. Determinar quais dos seguintes conjuntos são *sistemas reduzidos de restos módulo* 18:

(a) $\{1,5,25,125,625,3125\}$

(b) $\{5,11,17,23,29,35\}$

(c) $\{1,25,49,121,169,289\}$

(d) $\{1,5,7,11,13,17\}$

105. Sabendo que $k \equiv 16 \pmod{11}$, achar um inteiro $\underline{x}$, com $0 \leqslant x \leqslant 10$, tal que $k^3 + 6k^2 - 24 \equiv x \pmod{11}$.

106. Mostrar que, se o $mdc(a,2) = 1$, então $a^2 \equiv 1 \pmod{4}$.

107. Mostrar que o $mdc(a,mmc(b,c)) = mmc(mdc(a,b),mdc(a,c))$.

108. Calcular o *resto* da divisão de 314^{164} por 165.

109. Demonstrar que, se $\phi(2n) = \phi(3n)$, então $n = 2^k.a$, onde $\underline{a}$ é um inteiro tal que o $mdc(a,3) = 1$.

110. Sabendo que $(aa)_b$ no sistema decimal (base 10) escreve-se 34, calcular $\underline{a}$ e $\underline{b}$.

111. Savendo que $(aaa)_b$ no sistema decimal (base 10) escreve-se 1842, calcular $\underline{a}$ e $\underline{b}$.

112. Mostrar que, se $m > 1$ é ímpar, então $3 \mid (2^m+1)$, isto é, 2^m+1 é *composto*.

113. Demonstrar que para $n \geqslant 1$:

(a) $\binom{n}{k} < \binom{n}{k+1}$ se e somente se $0 \leqslant k < (n-1)/2$

(b) $\binom{n}{k} = \binom{n}{k+1}$ se e somente se $\underline{n}$ é *ímpar* e $k = (n-1)/2$.

114. Mostrar que, se $2 \leqslant k \leqslant n-2$, $n \geqslant 4$, então:

$$\binom{n}{k} = \binom{n-2}{k-2} + 2\binom{n-2}{k-1} + \binom{n-2}{k}.$$

115. Mostrar que, se $p \nmid n$ para todos os primos $p \leqslant \sqrt[3]{n}$, então $\underline{n}$ é primo ou é o produto de dois primos.

116. Mostrar que, se um inteiro $\underline{a}$ é ao mesmo tempo um *quadrado* e um *cubo*, então $a \equiv 0,1,9$ ou $28 \pmod{36}$.

117. Um inteiro compreendido entre 1 e 1200 deixa os restos 1, 2 e 6 quando dividido por 9,11 e 13, respectivamente. Achar esse inteiro.

118. Os inteiros $\underline{a}$ e $\underline{b}$ não são divisíveis pelo primo $\underline{p}$. Demonstrar:

(a) Se $a^p \equiv b^p \pmod{p}$, então $a \equiv b \pmod{p}$.

(b) Se $a^p \equiv b^p \pmod{p}$, então $a^p \equiv b^p \pmod{p^2}$.

119. Usando o *teorema de FERMAT*, demonstrar que, se $\underline{p}$ é um *primo ímpar*, então:

(a) $1^{p-1} + 2^{p-1} + 3^{p-1} + \ldots + (p-1)^{p-1} \equiv -1 \pmod{p}$

(b) $1^p + 2^p + 3^p + \ldots + (p-1)^p \equiv 0 \pmod{p}$

120. Demonstrar que um inteiro $n > 1$ é *primo* se e somente se $(n-2)! \equiv 1 \pmod{n}$.

121. Mostrar que, se $\underline{n}$ é um inteiro *composto*, então $(n-1)! \equiv 0 \pmod{n}$, exceto quando $n = 4$.

122. A sequência de inteiros

$$L_1, L_2, L_3, \ldots, L_{n-1}, L_n, \ldots$$

no caso em que

$$L_1 = 1,\ L_2 = 3 \quad e \quad L_n = L_{n-1} + L_{n-2} \ (n \geq 3)$$

isto é, a sequência:

$$1, 3, 4, 7, 11, 18, 29, \ldots$$

chama-se *sequência de LUCAS*. Demonstrar:

(a) L_{3n} é par e L_{3n-2} e L_{3n-1} são ímpares, para todo $n \geq 1$.

(b) $L_n F_n = F_{2n}$

(c) $L_1 + 2L_2 + 4L_3 + 8L_4 + \ldots + 2^{n-1}L_n = 2^n F_{n+1} - 1$

123. Determinar a mais elevada potência de 7 que divide o produto dos 1000 primeiros inteiros positivos.

124. Demonstrar que 60 divide o produto $(n^2-1)n^2(n^2+1)$, qualquer que seja o inteiro positivo n.

125. O inteiro $n = 2^x.3^y.5^z$. Calcular os expoentes x, y e z sabendo que o quociente n/2 tem 252 divisores e que os quocientes n/3 e n/5 tem, respectivamente, 45 divisores a menos que n.

126. Achar o menor inteiro positivo que tem 20 divisores positivos, sendo primos apenas 3, 5 e 7.

127. Determinar o inteiro $n = 2^x.3^y$, sabendo que o número de divisores de n^2 é o *triplo* do número de divisores de n.

128. Determinar a mais elevada potência de 11 que divide o produto:

$$P = 100 \times 101 \times 102 \times \ldots \times 1000$$

129. Os inteiros a e b são formados: o primeiro de 2m algarismos iguais a 1, e o segundo de m algarismos iguais a 4. Demonstrar que a soma $a + b + 1$ é um inteiro quadrado perfeito.

130. Verificar as igualdades:

(a) $100001^2 = 10^{10} + 2 \times 10^5 + 1$

(b) $99999^2 = 10^{10} - 2 \times 10^5 + 1$

(c) $100001 \times 99999 = 10^{10} - 1$

131. Demonstrar que o inteiro $n = 111\ldots12888\ldots896$, que tem n algarismos iguais a 1 e n-1 algarismos iguais a 8, é um quadrado perfeito.

132. Achar o *menor* inteiro positivo que admite: (a) 9 divisores positivos;

(b) 12 divisores positivos;

(c) 15 divisores positivos;

(d) 18 divisores positivos;

(e) 20 divisores positivos;

(f) 24 divisores positivos.

133. Mostrar que um inteiro da forma 4^{2n+1} *nunca é primo*.

134. Determinar o inteiro cujo produto de todos os seus divisores é igual a $3^{30} \times 5^{40}$.

135. Forma-se a sequência de inteiros:

49, 4489, 444889, 44448889, ...

na qual cada termo resulta de intercalar 48 no *centro* do anterior. Mostrar que todos os termos desta sequência são *quadrados perfeitos* e determinar a raiz quadrada do n-ésimo termo.

136. Determinar a *base* do sistema de numeração no qual o inteiro 16000 se escreve 1003000.

137. Achar um inteiro $\underline{n}$ tal que $n^2 + 49$ seja um quadrado perfeito.

138. Achar um inteiro de três algarismos que seja quadrado perfeito e divisível por 3 e por 5.

139. Demonstrar que, se os inteiros $\underline{a}$ e $\underline{b}$ são ímpares, então $a^2 + b^2$ não pode ser um quadrado perfeito.

140. Demonstrar que, se os inteiros $\underline{a}$ e $\underline{b}$ são primos com 3, então $a^2 + b^2$ não pode ser um quadrado perfeito.

141. Demonstrar que $\sum_{j=1}^{n} 1/j$ não é um inteiro para todo $n > 1$.

142. Demonstrar que $\sum_{j=1}^{n} 1/(2j-1)$ não é um inteiro para todo $n > 1$.

143. Demonstrar que, se os inteiros $\underline{a}$ e $\underline{b}$ são ímpares, então $a^2 + b^2$ é par, mas não é divisível por 4.

144. Demonstrar que, se o $mdc(n,7) = 1$, então $7|(n^6 - 1)$ e $7|(n^{12} - 1)$.

145. Achar o menor inteiro positivo $\underline{n}$ tal que

$$13|(n^2 + 1).$$

146. Caracterizar os inteiros positivos $\underline{n}$ para os quais se tem:

(a) $\phi(2n) = \phi(n)$. (b) $\phi(2n) > \phi(n)$

147. Demonstrar que, se $\underline{n}$ e $\underline{k}$ são inteiros positivos, então o número de inteiros positivos $\leqslant nk$ que são primos com $\underline{n}$ é igual a $k\phi(n)$.

148. Demonstrar que, se $\phi(m) = \phi(mn)$ e $n > 1$, então $n=2$ e $\underline{m}$ é *ímpar*.

149. Demonstrar que, se $d|n$, com $0 < d < n$, então $n - \phi(n) > d - \phi(d)$.

150. Achar o *resto* da divisão de $(12371^{56} + 34)^{28}$ por 111.

151. Demonstrar que $\phi(3n) = 2\phi(n)$ se e somente se 3 não divide $\underline{n}$ $(3 \nmid n)$.

152. Mostrar que todo inteiro *composto* menor que 1000 tem um fator primo menor que 37.

RESPOSTAS DOS EXERCÍCIOS

CAPÍTULO 1

1. $n(n + 1)/2$
2. $n = 2$
3. $n = 3$
4. $n = 4,5,7$
5. Falso: $(3.2)! \neq 3!2!$ e $(3 + 2)! \neq 3! + 2!$
8. $565 = 109 + 111 + 113 + 115 + 117$
9. $x=2, y=6$; $x=5, y=3$; $x=3, y=4$
10. 12, 24, 36 e 48
11. 10^{n-1} e $10^n - 1$
12. $x = 7$
13. $x = 1$ ou $x = 2$
15. $x = 23, y = 21$; $x = 13, y = 9$
17. (a) $3976 + 2934 + 5928$

    (b) $5623 + 4035 + 1269 = 11927$
18. (a) $13256 - 4310 = 8946$

    (b) $6321 - 435 = 5886$
19. 234
20. 9885
21. (a) 435.36 ; (b) 2403.62
22. 110997
23. 888889

24. 690

25. (a) 73 x 32 + 45; (b) 257 x 6 + 59

27. 14 e 56

CAPÍTULO 3

1. (a) 363 (b) 30 (c) 68 (d) 746

2. (a) 336 (b) 125 (c) 302400 (d) $315/2^{22}$

3. (a) $\sum_{i=1}^{4} a_i b_{i+1}$ (b) $\sum_{i=3}^{k} i(i+1)(i+2)$

(c) $\sum_{j=1}^{5} a_{2j} b_{j3}$

4. (a) V (b) F (c) V (d) F

7. (a) $t_6 = 21$ e $t_5 = 15$

(b) $t_3 = 6$, $t_4 = 10$ e $t_5 = 15$

(c) $t_5 = 15$, $t_6 = 21$ e $t_7 = 28$

9. 672

10. n = 9

CAPÍTULO 4

3. Falso: $6|(5+7)$, mas $6 \nmid 5$ e $6 \nmid 7$

14. 18, 38, 60 e 84

15. a = 6, b = 10 e c = 21

16. Falso: $6|18$ e $9|18$, mas $6 \nmid 9$
19. $b = 33, 34, 35$ e $r = 31, 19, 7$
20. 249 e 2; 166 e 3; 83 e 6
21. 322 e 19
22. 40, 80 e 120

CAPÍTULO 5

1. (a) 11 (b) 7 (c) 1
2. 1, 3 e 5
3. $X = \{1,5\}$
4. $a = -13$ ou $a = 13$
5. $c = mdc(22, 55) = 11$
6. 1
7. (a) 2 (b) 1
8. 1, 2, 5 e 10
9. 1 ou 3
13. 1 ou 2
14. 10, 50, 70 ou 110
15. $mdc(160 - 7, 198 - 11, 370 - 13) = 17$
16. (a) $a = 9$ e $b = 54$; $a = 18$ e $b = 45$; $a = 27$ e $b = 36$
    (b) $a = 6$ e $b = 126$; $a = 18$ e $b = 42$
17. $n = 48$ ou $n = 96$

CAPÍTULO 6

1. (a) 9 (b) 17 (c) 68 (d) 3 (e) 77 (f) 42

2. (a) 6 (b) 15 (c) 1 (d) 23

3. (a) $x = 4$, $y = -3$ (b) $x = 6$, $y = -1$
   (c) $x = 7$, $y = -3$ (d) $x = 39$, $y = -29$

4. (a) $x = 7$, $y = -17$ (b) $x = 1$, $y = -1$
   (c) $x = 56$, $y = -91$ (d) $x = 40$, $y = -64$
   (e) $x = -3$, $y = 17$ (f) não existem
   (g) $x = 3$, $y = -6$ (h) $x = 4$, $y = -14$

5. (a) $x = 28$, $y = -16$, $z = -1$
   (b) $x = 17$, $y = -153$, $z = -1$
   (c) $x = 18$, $y = -18$, $z = -3$
   (d) não existem

6. $x = 171$, $y = -144$, $z = -2$

7. (a) 315 (b) 5644 (c) 1320 (d) 6106 (e) 1344
   (f) 16731 (g) 32461 (h) 22338

8. $a = 184$ e $b = 72$

9. (a) $a = 12$ e $b = 336$; $a = 48$ e $b = 84$
   (b) $a = 8$ e $b = 560$; $a = 16$ e $b = 280$
   $a = 40$ e $b = 112$; $a = 56$ e $b = 80$
   (c) $a = 57$ e $b = 532$; $a = 217$ e $b = 372$

CAPÍTULO 7

1. 2, 7, 23, 47 e 79
2. $81 = 3 + 5 + 73$; $125 = 5 + 13 + 107$
3. 2 e 5
4. 3

5. 7

6. $n = 3$

7. $p = 5$

8. (a) 169 é *composto* (b) 197 é *primo*
   (c) 239 é *primo* (d) 473 é *composto*

9. $5040 = 2^4.3^2.5.7$

10. $mdc(a,b) = 2^6.19.23^3$

    $mmc(a,b) = 2^{30}.3.5^{21}.7^4.11^2.19^5.23^7$

12. 419 e 421; 431 e 433; 461 e 463

13. $5! + 2$, $5! + 3$, $5! + 4$, $5! + 5$

14. $101! + 2$, $101! + 3$, $101! + 4$, ..., $101! + 101$

15. (a) $32 = 3 + 29 = 13 + 19$
    (b) $100 = 3 + 97 = 11 + 89 = 17 + 83 = \ldots$
    (c) $456 = 7 + 449 = 13 + 443 = 17 + 439 = \ldots$
    (d) $1024 = 3 + 1021 = 5 + 1019 = 11 + 1013 = \ldots$

17. $n = 29$

19. $mdc(507, 1287) = 39$; $mmc(507, 1287) = 16731$

21. 930

22. Todos os *primos* ≤ 47.

CAPÍTULO 8

1. (a) $x = 20 + 9t$, $y = -15 - 7t$
   (b) $x = 18 + 23t$, $y = -3 - 4t$

(c) $x = -18 + 7t, \quad y = 45 - 17t$

(d) $x = 54 - 73t, \quad y = 10 - 14t$

(e) $x = -5 + 7t, \quad y = 35 - 48t$

(f) Não tem soluções inteiras

(g) $x = 11 + 30t, \quad y = -3 - 11t$

(h) $x = 2 + 2t, \quad y = 3t$

(i) $x = 7t, \quad y = -3 - 13t$

(j) Não tem soluções inteiras

(k) $x = 4t, \quad y = -6 + 7t$

(l) $x = 10 + 54t, \quad y = -3 - 17t$

2. (a) $x = 8 + 11t, \quad y = 1 + 5t$, onde $t \geqslant 0$

(b) Não tem soluções inteiras e positivas

(c) $x = 8 + 3t, \quad y = 2 + 2t$, onde $t \geqslant 0$

(d) $x = 1, \quad y = 66; \quad x = 12, \quad y = 4$

(e) Não tem soluções inteiras e positivas

(f) $x = 2, y = 38; x = 9, y = 20; x = 16, y = 2$

(g) Não tem soluções inteiras e positivas

(h) $x = 17 - 57t, \quad y = 47 - 158t$, onde $t \leqslant 0$

3. 118

4. $100 = 56 + 44$

5. 8/13 e 13/17

CAPÍTULO 9

1. (a) V (b) V (c) F (d) V (e) F (f) F

2. (a) V (b) V

3. (a) 5 (b) 1

4. 1,2,5,10,71,142,355,710

5. $n \equiv 1 \pmod{2}$; $n = 2k + 1$; n deixa o *resto* 1 na divisão por 2

6. 2, 7 e 12

7. 7, 24,41, 58, 75 e 92

9. $7^2 \equiv 5^2 \pmod{8}$ e $7 \not\equiv 5 \pmod{8}$

14. 4 e 6

19. (a) e (c)

20. (b), (c) e (d)

21. { 2,3,5,7,11,13,29} ; existem outros.

22. { 0,4,8,12,16,20,24 }

CAPÍTULO 10

1. (a) $x \equiv 9 \pmod{17}$ (b) $x \equiv 6 \pmod{17}$

   (c) $x \equiv 2,8,14 \pmod{18}$ (d) $x \equiv 18 \pmod{29}$

   (e) $x \equiv 16 \pmod{26}$ (f) $x \equiv 6,13,20 \pmod{21}$

   (g) Não tem soluções (h) $x \equiv 45,94 \pmod{98}$

   (i) $x \equiv 2,5,8,11 \pmod{12}$ (j) $x \equiv 6,30 \pmod{48}$

2. (a) $x = 15 + 51t$, $y = -1 + 4t$

   (b) $x = 13 + 25t$, $y = 7 - 12t$

   (c) $x = 14 + 53t$, $y = 1 + 5t$

   (d) $x = 3 + 6t$, $y = -2 - 7t$

(e) $x = 20 + 27t, \quad y = -8 - 11t$

(f) $x = 42 + 131t, \quad y = 24 + 75t$

(g) $x = 2t, \quad y = 4 - 3t$

(h) $x = 8 + 11t, \quad y = 37 + 61t$

(i) $x = 9 + 77t, \quad y = -5 - 65t$

(j) $x = 2 + 5t, \quad y = 11 - 3t$

3. (a) 3 (b) 1 (c) 5 (d) 0

4. 0, 1, 2, 4, 5, 10 ou 20

CAPÍTULO 11

1. (a) $x \equiv 1 \pmod{6}$

   (b) $x \equiv 197 \pmod{228}$

   (c) $x \equiv 242 \pmod{858}$

2. (a) $x \equiv 348 \pmod{385}$ (b) $x \equiv 52 \pmod{105}$

   (c) $x \equiv 785 \pmod{1122}$ (d) $x \equiv 4944 \pmod{9889}$

   (e) $x \equiv 106 \pmod{252}$ (f) $x \equiv -1 \pmod{9889}$

   (g) $x \equiv 40a - 24b - 15c \pmod{120}$

3. (a) $x \equiv 12113 \pmod{20128}$

   (b) $x \equiv 1423 \pmod{2310}$

4. (a) $x \equiv 26 \pmod{63}$

   (b) $x \equiv 148 \pmod{210}$

   (c) $x \equiv 33 \pmod{276}$

CAPÍTULO 13

1. 4, 6 e 8
2. 8, 20, 24 e 12
3. (a) 15 (b) 24 (c) 2 (d) 24
4. 50
5. 12
6. 24
7. 6300
8. 3150
9. $1 + p + q + pq$, $1 + p + p^2 + p^3$

   $1 + p + q + p^2 + pq + p^2q$
10. 744, 1344, 3224, 14736
11. (a) 403 (b) 1170 (c) 1010 (d) 15960
12. 24 e 39
18. 5040, 7920 e 9360
19. 1, 7, 13, 49, 91 e 637
20. 25, 30, 50, 75 e 150
21. $n = 432$
22. $n = 1400$
23. (a) $x = 22$; (b) $x = 38, 24, 59$

CAPÍTULO 15

1. 96, 720, 1152 e 2160
2. 4 e 2
3. p

10. (a) $x \equiv 11 \pmod{12}$ (b) $x \equiv 6 \pmod{9}$
    (c) $x \equiv 3 \pmod{10}$ (d) $x \equiv 3 \pmod{5}$
    (e) $x \equiv 9 \pmod{17}$ (f) $x \equiv 1 \pmod{8}$

CAPÍTULO 16

1. $130816 = 2^8(2^9 - 1)$, e como $2^9 - 1 = 7.73$ não é um *primo*, segue-se que 130816 não é um número perfeito.

2. $2^{11} - 1 = 23.89$ não é um *primo*. Logo, n não é um número perfeito.

9. 56

11. $s(120) = 3.120$ e $s(672) = 3.672$

17. 12, 18 e 20 são *abundantes*, 6 é *perfeito* e os demais inteiros são *deficientes*.

18. $25575 = 3^6.5.7$

24. $M_{19} = 524287$

25. $23|M_{11}$ e $233|M_{29}$

CAPÍTULO 17

1. $F_{15} = 610$, $F_{18} = 2584$, $F_{20} = 6765$

2. $F_{17} - 1 = 1596$

3. $F_{24} = 46368$

4. $F_{21} - 1 = 10945$

5. $(-1)^{18}F_{16} + 1 = 988$

6. $F_{14}F_{15} = 229970$

7. $F_1 = 1$ e $F_9 = 34$

8. $F_5 = 5$ e $F_{12} = 144$

9. $F_1, F_2, F_3, F_4, F_6, F_{12}$

10. $F_1, F_2, F_4, F_8, F_{10}$

11. $50 = F_4 + F_7 + F_9$

    $75 = F_3 + F_5 + F_7 + F_{10}$

    $100 = F_1 + F_3 + F_6 + F_{11}$

22. $F_{11} = 2F_9 + F_8$, $F_{12} = 6F_8 + (F_8 - F_4)$

CAPÍTULO 18

1. (7,24,25), (11,60,61), (17,144,145)

2. (a) (48,20,52); (b) (126,32,130)

3. $b = 180$ e $c = 181$
4. $b = 21$ e $c = 29$
5. (5,12,13), (7,24,25), (9,40,41)
6. (16,12,20), (16,63,65), (16,30,39)
7. (16,30,34), (72,30,78), (40,30,50), (224,30,226)
8. (40,9,41), (40,399,401)
9. (60,11,61), (60,91,109), (60,221,229), (60,899,901)

CAPÍTULO 19

1. $(-5)_8 = \{\ldots, -21, -13, -5, 3, 11, \ldots\}$
2. $1913_9 = 5_9 = \{\ldots, -13, -4, 5, 14, 23, \ldots\}$
3. $m = 1, 7$
4. $m = 1, 2, 3, 4, 6, 12$

CAPÍTULO 20

1. 890 e 7885
2. 421, 1107, 4159
3. $(204)_8$, $(435)_8$
4. $(10111010100)_2$, $(2001021)_3$, $(4226)_7$, $(2037)_9$, $(1137)_{11}$
5. $(112010)_5$, $(4223)_7$
6. $x = 102$, $x = 153$, $x = 7$

7. $(34132)_5$, $(4531)_7$

8. 5

9. 20

10. 6763

11.

+	0	1
0	0	1
1	1	10

x	0	1
0	0	0
1	0	1

12. 374518 não é divisível por 9 ($9 \nmid 28$)

1520397 é divisível por 9 ($9|27$)

13. 370546 é divisível por 11 ($11|11$)

22481907 não é divisível por 11 ($11 \nmid 19$)

14. 176521221 é divisível por 9 ($9|27$) e não é divisível por 11 ($11 \nmid -3$)

149235678 é divisível por 9 ($9|45$) e não é divisível por 11 ($11 \nmid 9$)

17. (a) $x = 4$; (b) $x = 0,3,6,9$; (c) $x = 5$

(d) $x = 2,8$; (e) $x = 4$

19. (a) $x = 6$, $y = 5$; $x = 1$, $y = 0$

(b) $x = 7$, $y = 0$; $x = 3$, $y = 4$; $x = y = 8$

(c) $x = 4$, $y = 0$; (d) $x = 6$, $y = 4$

(e) $x = 3$, $y = 0$; $x = 7$, $y = 5$

(f) $x = 0$, $y = 8$; $x = 8$, $y = 0$

20. $abc - cba = (c + 10b + 100a) - (a + 10b + 100c)$

$= 99(a - c) = 11 \times 9(a - c)$

21. $aaa = (1 + 10 + 100) \times a = 111 \times a = 37 \times 3 \times a$

22. $(2 \times ab)ab = 2 \times ab \times 100 + ab = 201 \times ab = 67 \times 3 \times ab$

24. (a) $x = 1, y = 8$; $x = 2, y = 4$

$x = 5, y = 4$; $x = 7, y = 8$; $x = 8, y = 4$

(b) $x = 2,5,8, y = 0$; $x = 0,3,6,9, y = 5$

(c) $x = 8, y = 0$; $x = 1, y = 4$; $x = 4, y = 7$

(d) $x = 0, y = 8$; $x = 8, y = 0$

(e) $x = 3, y = 2$; $x = 6, y = 8$

(f) $x = 1, y = 2$

25. $aaaaaa = (1 + 10 + 10^2 + 10^3 + 10^4 + 10^5) \times a =$

$= 111111 \times a = 3 \times 7 \times 11 \times 13 \times 37 \times a$

26. $ab + ba + ac + ca + bc + cb = b + 10a + a + 10b + c +$

$+ 10a + a + 10c + c + 10b + b + 10c =$

$= 22a + 22b + 22c = 22\ (a + b + c)$

CAPÍTULO 21

1. (a) 8, 16, 16
   (b) 18, 18, 9
   (c) 11, 11, 22

2. 4, 2, 4, 4, 2, 4, 2

3. 6 e 26

9. 3 e 7

10. 5, 6, 7, 10, 11, 12, 14

11. 3, 10, 13, 14, 15

12. 2 e 3; 2 e 5; 2,6,7,e 8; 2,6,7 e 11

EXERCÍCIOS SUPLEMENTARES

21. 89

22. $x = 4$ e $y = 9$

23. $a = 62$

24. (a) 17; (b) 59; (c) 1103

29. 1

40. $n = 213$

41. 3

42. 1

44. $n = 5, 8, 12$

47. Todo inteiro $k \geqslant 3$

50. 17

53. $6^2 = t_8$, $35^2 = t_{49}$, $204^2 = t_{288}$

54. 71

55. p^9 e p^4q; $48 = 2^4.3$

56. (a) $n = 17,32,34,40,48,60$

(b) $n = 35,39,45,52,56,70,72,78,84,90$

(c) $n = 31,62$

59. Somente o conjunto (c)

62. $n = 33$

67. (a) 0, -13, 0, -15, 0

(b) $-p$

(c) 0

(d) $-p^k$

73. $p - 2$ e $p^2 - 2p$

88. $(10^{n+1} - 9n - 10)/81$

89. 2^n

90. 13

91. 5

92. (a) $a = 8$, $b = 4$; (b) $a = 2$, $b = 5$

94. $x = 250$, $y = 249$

95. $n = 1800$

96. 238, 476, 714 e 952

97. $n = 6, 12, 24, 30, 42, 48$

98. $n = 45, 90, 180$

99. 128

103. Todos

104. (a) e (d)

105. $x = 9$

108. 101

110. $a = 2$, $b = 16$, ou $a = 1$, $b = 33$

111. $a = 6$, $b = 17$

117. 838

123. 7^{164}

125. $x = 4$, $y = 6$, $z = 8$

126. 2835

127. $n=324$ ou $n=144$

128. 11^{89}

132. (a) 36 (b) 60 (c) 144
(d) 180 (e) 240 (f) 360

134. 16875

135. $(2 \times 10^n + 1)/3 = (666...67)$

136. 5

137. $n = 24$

138. 225 e 900

BIBLIOGRAFIA

1. ARMENDARIZ,E. e McADAM,S.
   Elementary Number Theory; Macmillan; 1980

2. ANDREWS,G.E.
   Number Theory; Saunders; 1971

3. ADAMS,W.W. e GOLDSTEIN,L.J.
   Introduction to Number Theory; Prentice-Hall; 1976

4. APOSTOL,T.M.
   Introducción a la Teoria Analítica de Números; Reverté; 1980

5. BURTON,D.M.
   Elementary Number Theory; Allyn and Bacon; 1976

6. BEILER,A.H.
   Recreations in the Theory of Numbers; Dover; 1966

7. DUDLEY,U.
   Elementary Number Theory; Freeman; 1978

8. DANTZIG,T.
   Número: A Linguagem da Ciência; Zahar; 1970

9. HARDY,G.H. e WRIGHT,E.M.
   Introduction to Theory of Numbers; Oxford; 1979

10. ITARD, J.

Arithmétique et Théorie des Nombres; P.U. F.; 1973

11. LeVEQUE, W.J.

Fundamentals of Number Theory; Addison-Wesley; 1977

12. NIVEN, I. e ZUCKERMAN, H.

Introduccion a la Teoria de los Números; Limusa; 1976

13. PETTOFREZZO, A. e BYRKIT, D.

Introduccion a la Teoria de los Números; Prentice-Hall; 1972

14. VOROBYOV, N.

Los Números de FIBONACCI; Limusa; 1973

15. VINOGRADOV, I.

Fundamentos de la Teoria de los Números; Mir; 1977