CAPÍTULO 6

ALGORÍTMO DE EUCLIDES MÍNIMO MÚLTIPLO COMUM

Lema 6.1 Se a = bq + r, então o mdc(a,b) = mdc(b,r).

Demonstração:

Se o mdc(a,b) = d, então d|a e d|b, o que implica d|(a - bq) ou d|r, isto é, d é um *divisor comum* de b e r (d|b e d|r).

Por outro lado, se c é um *divisor comum* qualquer de b e r (c|b e c|r), então c|(bq + r) ou c|a, isto é, c é um *divisor comum* de a e b, o que implica c ⩽ d. Assim sendo, o mdc(b,r) = d.

6.1 ALGORITMO DE EUCLIDES

Sejam a e b dois inteiros não conjuntamente nulos (a≠0 ou b≠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 a e b são inteiros positivos *distintos*, p.ex., com $a > b$, tais que b *não divide* 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 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:

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

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.

Exemplo 6.2 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 $x = -2$ e $y = -3$, 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:

$$36 = 252(-2 + 180) + (-180)(-3 + 252) =$$

$$= 252.178 + (-180)249$$

Exemplo 6.3 O mdc de dois inteiros positivos a e b é 74 e na sua determinação pelo *algoritmo de EUCLIDES* os quocientes obtidos foram 1, 2, 2, 5, 1 e 3. Calcular a e b.

	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:

$$ak = (bk)q_1 + r_1k, \quad 0 < r_1k < bk$$

$$bk = (r_1k)q_2 + r_2k, \quad 0 < r_2k < r_1k$$

$$r_1k = (r_2k)q_3 + r_3k, \quad 0 < r_3k < r_2k$$

$$\cdots\cdots\cdots\cdots\cdots \qquad \cdots\cdots\cdots$$

$$r_{n-2}k = (r_{n-1}k)q_n + r_nk, \quad 0 < r_nk < r_{n-1}k$$

$$r_{n-1}k = (r_nk)q_{n+1} + 0$$

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:

$$\text{mdc}(ak, bk) = r_nk = k.\text{mdc}(a,b)$$

Assim, p.ex.:

$$\text{mdc}(12,30) = \text{mdc}(2.6, 5.6) = 6.\text{mdc}(2,5) = 6.1 = 6$$

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:

$$mdc(ak, bk) = mdc(-ak, -bk) =$$

$$= mdc(a.|k|, b.|k|) = |k|.\ mdc(a,b)$$

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:

$$M(a) = \{ x \in Z \mid a|x \} = \{ aq \mid q \in Z \}$$

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 a e de b indica se por M(a,b). Portanto, simbolicamente:

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

ou seja:

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

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 a e b, isto é: M(a,b) = M(b,a).

Obviamente, 0 é um *múltiplo comum* de a e b: $0 \in M(a,b)$. E os produtos ab e -(ab) também são *múltiplos comuns* de a e b.

Exemplo 6.4 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 $m \leqslant c$.

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 $\text{mmc}(a,b) \leqslant |ab|$.

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, ..., 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 $a \mid a(b/d)$ e $b \mid b(a/d)$, 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 ≤ 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) mdc(56, 72) = 56x + 72y

   (b) mdc(24, 138) = 24x + 138y

   (c) mdc(119, 272) = 119x + 272y

   (d) 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 $\frac{\text{mmc}(a,b)}{\text{mdc}(a,b)} = 84$.

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 $p|a_1a_2...a_n$, então existe um índice k, com $1 \leqslant k \leqslant n$, tal que $p|a_k$.

Demonstração:

Usando o "Teorema da induçao 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 $p|a_1a_2...a_n$, então

$$p|a_n \text{ ou } p|a_1a_2...a_{n-1}$$

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 "*Principio 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 $d \mid p$ e $p \mid a$, o que implica $d \mid a$, 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:

$$p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s$$

Com o mesmo raciocínio conclui-se que $p_2 = q_2$, o que implica:

$$p_3 p_4 \cdots p_r = q_3 q_4 \cdots q_s$$

e assim por diante.

Assím sendo, se subsiste a desigualdade $r < s$, então se chega necessariamente a igualdade:

$$1 = q_{r+1} q_{r+2} \cdots q_s$$

o que é *absurdo*, porque cada $q_j > 1$. Logo, $r = s$ e temos:

$$p_1 = q_1, \quad p_2 = q_2, \cdots, \quad p_r = q_r$$

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:

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

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:

$$P = p_1p_2p_3\cdots p_n + 1$$

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:

$$p|P \quad \text{e} \quad p|p_1p_2p_3\cdots p_n$$

o que implica:

$$p|P - p_1p_2p_3\cdots p_n \quad \text{ou} \quad p|1$$

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*.

Teorema 7.4 Se um inteiro positivo $a > 1$ é *composto*, então a possui um *divisor primo* $p \leqslant \sqrt{a}$.

Demonstração:

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 b tem pelo menos um *divisor primo* p, 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 a.

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 a 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,...,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

Definição 7.2 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 grán des, 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:

$$5! + 2,\ 5! + 3,\ 5! + 4,\ 5! + 5$$

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

$$24, 25, 26, 27 \quad \text{e} \quad 32, 33, 34, 35$$

$$54, 55, 56, 57 \quad \text{e} \quad 74, 75, 76, 77$$

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 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 a e r (razão) são inteiros positivos *primos entre si*, há um número infinito de *primos* (DIRICHLET).

(ii) Para todo inteiro $n > 3$, entre n e $2(n-1)$ existe, pelo menos, um *primo* (TSCHEBISCHEFF).

7.8 MÉTODO DE FATORAÇÃO DE FERMAT

Dado um inteiro positivo *ímpar* n, a decomposição de 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 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	$21 + 1 = 22$
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 $8^n \neq 1$, com $n \geq 1$, é *composto*.

27. Mostrar que, se n^2+2 é *primo*, então $3 \mid n$.

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 $p \mid a^n$, então $p^n \mid a^n$.

    (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 $24 \mid (p^2 - q^2)$.

    (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 n é *composto*, então 2^{n-1} também é *composto*.

33. Demonstrar que, se o inteiro $n > 2$, então existe um *primo* p tal que $n < p < n!$.

34. Demonstrar que todo *primo ímpar* é da forma $4k+1$ ou $4k-1$, onde k é um inteiro positivo.