

1 Aritmética dos Inteiros

1.1 Lema da Divisão e o Algoritmo de Euclides

Recorde-se que $|a|$, o módulo ou valor absoluto de a , designa

$$|a| = \begin{cases} a & \text{se } a \in \mathbb{N} \\ -a & \text{se } a \notin \mathbb{N} \end{cases}$$

Dados $a, b \in \mathbb{Z}$ denotamos por

$$a \mid b :$$

a divide b ou a é um **divisor** de b , a relação definida por

$$a \mid b \iff \exists q \in \mathbb{Z} : b = aq$$

Da definição decorrem imediatamente as seguintes propriedades:

1. $a \mid b$ e $b \mid c \implies a \mid c$
2. $a \mid b$ e $a \mid c \implies a \mid (b + c)$
3. $a \mid b \implies a \mid bs, \forall s \in \mathbb{Z}$
4. $a = bq + r, d \mid a, d \mid b \implies d \mid r$
5. $a \mid b \iff |a| \mid |b|$

Lema 1.1 da Divisão (inteira):

Dados $b \in \mathbb{N} \setminus 0$ e $a \in \mathbb{Z}$, existem $q, r \in \mathbb{Z}$ **únicos**, tais que

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

Demonstração 1.2 *De facto, o resto r pode ser definido como o menor elemento do conjunto, obviamente não vazio,*

$$X = \{a - bx \mid x \in \mathbb{Z}\} \cap \mathbb{N},$$

e definir q como o inteiro que satisfaz $a - bq = r$.

Notamos em primeiro lugar que $0 \leq r$, pela definição do conjunto X ; e se $r \geq b$, ou seja, se existisse $s \geq 0$ tal que $r = b + s$, então teríamos

$$a = bq + r = b(q + 1) + s$$

e portanto teríamos $s \in X$ mas $s < r$, em contradição com o facto de r ser o menor elemento deste conjunto.

Além disso, r é o único elemento de X menor que b : se r' é outro elemento de X , $r' = a - bq'$ temos $r' = bq + r - bq'$ e portanto $r' - r = b(q - q')$; como $r' > r$ temos $q - q' > 0$, logo $r' = r + b(q - q') \geq b(q - q') \geq b$.

Notação 1.3 (Knuth): *q é o maior inteiro menor ou igual a $\frac{a}{b}$, representado na notação introduzida por D. Knuth como $q = \left\lfloor \frac{a}{b} \right\rfloor$.*

Teorema 1.4 (Representação dos inteiros em bases):

Seja b um inteiro ≥ 2 . Então qualquer inteiro positivo a pode ser representado na base b , isto é, a pode ser escrito de forma única como

$$a = r_n b^n + r_{n-1} b^{n-1} + \dots + r_2 b^2 + r_1 b + r_0$$

com $0 \leq r_i < b; i = 1, 2, \dots, n$.

Notação 1.5 *Escreve-se então $a = (r_n r_{n-1} \dots r_2 r_1 r_0)_b$.*

Demonstração 1.6 *A demonstração é uma simples aplicação do Lema da Divisão e do Princípio de Indução Finita (Forte): em primeiro lugar, 1 tem a representação, obviamente única, dada por $r_0 = 1$.*

Suponhamos como hipótese de indução que para todo o $1 \leq m < n$ existe uma representação única na base b ; pelo Lema da Divisão $n = qb + r_0$ com $0 \leq r_0 < b$; como $q < n$ temos

$$q = s_{k-1}b^{k-1} + \dots + s_0$$

para algum $0 < k$ e $0 \leq s_i < b$, unicamente determinados, pelo que

$$n = r_k b^k + \dots + r_1 b + r_0$$

definindo $r_i = s_{i-1}$ para todo o $0 < i \leq k$. Esta representação é única: se $n = t_j b^j + \dots + t_1 b + t_0$, com $0 \leq t_i < b$, temos em primeiro lugar que, pelo Lema da Divisão, $t_0 = r_0$; mas então

$$t_j b^j + \dots + t_1 b = r_k b^k + \dots + r_1 b$$

e portanto

$$t_j b^{j-1} + \dots + t_1 = r_k b^{k-1} + \dots + r_1 = q$$

e como por hipótese de indução a representação é única para todo o $1 \leq m < n$, temos $j = k$ e $t_i = r_i$ para todo o i .

O raciocínio feito na demonstração indica um algoritmo para determinar a representação na base b de a :

Exemplo 1.7 *Sejam, por exemplo, $b = 6$ e $a = 347$; temos sucessivamente*

$$\begin{aligned} 347 &= 57 \times 6 + 5 = \\ &= (9 \times 6 + 3) \times 6 + 5 = 9 \times 6^2 + 3 \times 6 + 5 = \\ &= (1 \times 6 + 3) \times 6^2 + 3 \times 6 + 5 = 6^3 + 3 \times 6^2 + 3 \times 6 + 5 \end{aligned}$$

e portanto, usando a notação introduzida acima $347 = (1335)_6$.

Exercícios II.1

1. Calcular a representação de 29674 na base 3 e na base 11.
2. Considere-se o seguinte algoritmo: dados naturais $a \leq b$ constrói-se uma tabela com a no topo da primeira coluna e b no topo da segunda. Em cada passo, preenchemos uma nova linha, escrevendo na primeira coluna o quociente da divisão da entrada anterior na mesma coluna, por 2, e na segunda o dobro da entrada anterior. Terminamos quando a entrada na primeira coluna for 1. A tabela seguinte ilustra o procedimento para $a = 345$ e $b = 512$:

345	512
172	1024
86	2048
43	4096
21	8192
10	16384
5	32768
2	65536
1	131072

Em seguida, somamos as entradas da segunda coluna que têm à esquerda um número ímpar; no nosso caso

$$512 + 4096 + 8192 + 32768 + 131072 = 176640$$

que é o produto dos números iniciais $176640 = 345 \times 512$.

Explicar porque resulta este método primitivo de multiplicação (só é preciso saber somar e dividir e multiplicar por 2...)

1.2 Máximo Divisor Comum

Definição 1.8 Dados $a, b \in \mathbb{Z}$, não ambos nulos, diz-se que d é o **máximo divisor comum** de a e b , $d = \text{mdc}(a, b)$, se

(i) $d > 0$; (ii) $d \mid a$ e $d \mid b$; (iii) $c \mid a$ e $c \mid b \implies c \mid d$.

Nota 1.9 Temos obviamente

- $\forall a \in \mathbb{N} : mdc(a, 0) = a;$
- $\forall a \in \mathbb{N} : mdc(a, 1) = 1.$

Teorema 1.10 Dados $a, b \in \mathbb{Z}$, não ambos nulos, existe sempre o **máximo divisor comum** de a e b .

Este facto pode ser estabelecido teoricamente e resolvido na prática pelo

Algoritmo de Euclides para calcular $mdc(a, b); a, b \in \mathbb{N};$

- 1 Inicializar $u = a$ e $v = b;$
- 2 Enquanto $v > 0,$, calcular $u = qv + r$ com $0 \leq r < v$, substituir u por v e v por $r;$
- 3 Quando $v = 0,$ $u = mdc(a, b).$

Uma descrição mais detalhada, incluindo a justificação de que este procedimento pára num número finito de passos, é: Seja $r_{-1} = a$ e $r_0 = b;$ definimos por recorrência

$$r_{n-1} = q_{n+1}r_n + r_{n+1}$$

com $0 \leq r_{k+1} < r_k$ para $k \geq 1.$

r_k é uma sucessão estritamente decrescente de inteiros não negativos e portanto existe m tal que $r_{m+1} = 0;$ isso implica que $r_m \mid r_{m-1}$ e, por um raciocínio anaálogo ao do princípio de Indução Finita, deduzimos que $r_m \mid r_n$ para todo o $n \geq -1:$ se $r_m \mid r_k$ para todo o $k \geq n,$ então como

$$r_{n-1} = q_{n+1}r_n + r_{n+1}$$

tem que se ter $r_m \mid r_{n-1}.$

Portanto r_m é um divisor comum de a e $b;$ mas, por outro lado, se $c \mid a$ e $c \mid b,$ deduzimos da mesma forma que $c \mid r_n$ para todo o n e portanto $c \mid r_m.$ Concluimos que $r_m = mdc(a, b).$

Exemplo 1.11 seja $a = r_{-1} = 5324$ e $b = r_0 = 1023$; obtemos sucessivamente

$$r_{-1} = 5324 = 5 \times 1023 + 209 = q_1 r_0 + r_1$$

$$r_0 = 1023 = 4 \times 209 + 187 = q_2 r_1 + r_2$$

$$r_1 = 209 = 1 \times 187 + 22 = q_3 r_2 + r_3$$

$$r_2 = 187 = 8 \times 22 + 11 = q_4 r_3 + r_4$$

$$r_3 = 22 = 2 \times 11 + 0 = q_5 r_4 + r_5$$

Nota 1.12 O algoritmo de Euclides pode ser visto como um caso especial do **desenvolvimento em fracção contínua** de um número :

$$\frac{a}{b} = q_1 + \frac{r_1}{b} = q_1 + \frac{r_1}{q_2 r_1 + r_2} =$$

$$q_1 + \frac{1}{q_2 + \frac{r_2}{r_1}} = \dots = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{1}{\dots + \frac{1}{q_m + \frac{1}{q_{m+1}}}}}}$$

Corolário 1.13 Se $d = \text{mdc}(a, b)$, existem $x, y \in \mathbb{Z}$:

$$xa + yb = d.$$

Demonstração 1.14 Os coeficientes x, y podem ser obtidos por um procedimento análogo ao da demonstração anterior; se $d = r_m$, isso significa que

$$d = r_{m-2} - q_m r_{m-1};$$

mas como $r_{m-3} = q_{m-1} r_{m-2} + r_{m-1}$

$$d = r_{m-2} - q_m (r_{m-3} - q_{m-1} r_{m-2}) = -q_m r_{m-3} + (1 + q_m q_{m-1}) r_{m-2}$$

e assim por diante: se já temos

$$d = sr_n + tr_{n+1}$$

e

$$r_{n-1} = q_{n+1}r_n + r_{n+1}$$

então

$$d = sr_n + t(r_{n-1} - q_{n+1}r_n) = tr_{n-1} + (s - tq_{n+1})r_n$$

e continuando deste modo acabamos com uma equação

$$d = xa + yb.$$

Nota 1.15 Como se verifica facilmente, o $\text{mdc}(a, b)$ é o menor inteiro positivo que se pode escrever como combinação inteira de a e b .

Aliás, $\text{mdc}(a, b)$ pode ser definido como o menor elemento positivo do conjunto

$$\{as + bt : s, t \in \mathbb{Z}\}.$$

Esta definição dá relevo a certos aspectos da álgebra dos inteiros (que serão estudados noutras disciplinas) mas, por outro lado, não nos indica directamente um método de cálculo, como acontece com o algoritmo de Euclides.

O cálculo dos coeficientes x e y do corolário anterior pode ser feito, com vantagem, procedendo de outro modo: como, para todo o $n > 0$, se tem $r_n = r_{n-2} - q_n r_{n-1}$, se já tivermos

$$r_{n-2} = x_{n-2}a + y_{n-2}b, \text{ e do mesmo modo } r_{n-1} = x_{n-1}a + y_{n-1}b$$

então obtemos igualmente uma combinação

$$r_n = x_n a + y_n b = (x_{n-2} - q_n x_{n-1})a + (y_{n-2} - q_n y_{n-1})b.$$

Podemos portanto ir calculando os coeficientes x_k e y_k ao mesmo tempo que calculamos os sucessivos r_k e q_k e chegar ao fim da aplicação do algoritmo, obtendo como resultado final o $\text{mdc}(a, b)$ e os coeficientes x e y da equação. Esta versão do algoritmo é habitualmente chamada **Algoritmo de Euclides estendido**.

A tabela seguinte descreve a aplicação do algoritmo de Euclides estendido a $a = 2163$ e $b = 910$:

	r_i	q_i	x_i	y_i
	2163		1	0
	910		0	1
2163 = 2 × 910 + 343	343	2	1	-2
910 = 2 × 343 + 224	224	2	-2	5
343 = 1 × 224 + 119	119	1	3	-7
224 = 1 × 119 + 105	105	1	-5	12
119 = 1 × 105 + 14	14	1	8	-19
105 = 7 × 14 + 7	7	7	-61	145
14 = 2 × 7 + 0				

Nota 1.16 Estes cálculos podem também ser representados através do produto de matrizes: a equação acima pode escrever-se como

$$\begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix} \begin{pmatrix} x_{n-2} & y_{n-2} \\ x_{n-1} & y_{n-1} \end{pmatrix} = \begin{pmatrix} x_{n-1} & y_{n-1} \\ x_n & y_n \end{pmatrix};$$

com a condição inicial

$$r_{-1} = 1 \times a + 0 \times b = x_{-1}a + y_{-1}b$$

e

$$r_0 = 0 \times a + 1 \times b = x_0a + y_0b$$

temos que os coeficientes x e y pretendidos são os elementos da segunda linha da matriz

$$\begin{pmatrix} 0 & 1 \\ 1 & -q_m \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{m-1} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix}$$

Exercícios II.2

1. Calcular $d = \text{mdc}(a, b)$ e determinar os $x, y \in \mathbb{Z}$ tais que $d = ax + by$ nos casos seguintes:

a) $a = 721$ $b = 448$

b) $a = 341$ $b = 209$

c) $a = 2163$ $b = 922$

2. O menor múltiplo comum de dois números inteiros a, b define-se como o inteiro positivo $mmc(a, b)$ que é múltiplo de ambos e tal que

$$a|c \wedge b|c \implies mmc(a, b)|c$$

Mostrar que para a, b positivos se tem

$$mmc(a, b) = \frac{ab}{mdc(a, b)}$$

3. A definição de máximo divisor comum generaliza-se para qualquer conjunto finito de inteiros: se a_1, a_2, \dots, a_n são inteiros (não nulos) d é o seu máximo divisor comum se

$$\forall 1 \leq i \leq n \ d | a_i, \text{ e } (\forall 1 \leq i \leq n \ c | a_i) \implies c | d.$$

- a) Provar, por indução em n , que existe o máximo divisor comum de quaisquer $n > 2$ inteiros a_1, a_2, \dots, a_n , que se verifica a seguinte recorrência:

$$mdc(a_1, a_2, \dots, a_n) = mdc(mdc(a_1, a_2, \dots, a_{n-1}), a_n),$$

e que se $d = mdc(a_1, a_2, \dots, a_n)$, então existem inteiros x_1, x_2, \dots, x_n tais que

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

- b) A fórmula de recorrência através da qual se prova na alínea anterior a existência do mdc e a sua representação como combinação dos a_i com coeficientes inteiros, não é prática para o calcular, para n muito maior que 2 (se a usássemos para programar esse cálculo, teríamos um algoritmo recursivo).

Em alternativa, podemos chegar ao resultado assim: dados $n > 2$ inteiros a_1, a_2, \dots, a_n , definimos por recorrência a sucessão

$$d_1 = a_1, \quad d_{k+1} = mdc(d_k, a_{k+1}).$$

Provar, mais uma vez por indução em n , que d_n é o máximo divisor comum de a_1, a_2, \dots, a_n . Deste modo podemos calcular d os coeficientes x_i com menos cálculos do que pela fórmula anterior.

4. Neste exercício usamos a notação abreviada (a_1, a_2, \dots, a_n) para designar o máximo divisor comum dos inteiros a_1, a_2, \dots, a_n .
 O menor múltiplo comum é designado por $[a_1, a_2, \dots, a_n]$.
 Provar que se verificam as seguintes identidades ou dar um contra-exemplo:

- a) $(ma, mb) = m(a, b)$ e $[ma, mb] = m[a, b]$ para $m \in \mathbb{N}$;
- b) $((a, b), (a, c)) = (a, b, c)$ e $[[a, b], [a, c]] = [a, b, c]$;
- c) $(a, b)(c, d) = (ac, ad, bc, bd)$;
- d) se $(a, b) = (c, d)$ então $[a, b] = [c, d]$;
- e) se $(a, b) = (c, d)$ então $(a^2, b^2) = (c^2, d^2)$;
- f) $(ab, ac, b, c)[a, b, c] = abc$;

5. Mostrar que, dado um natural $a > 1$, se verifica

$$\text{mdc}(a^m - 1, a^n - 1) = a^{\text{mdc}(m, n)} - 1$$

Sugestão: verificar que se $m = qn + r$, com $0 \leq r < n$, então

$$a^m - 1 = a^r(1 + a^n + \dots + a^{(q-1)n})(a^n - 1) + a^r - 1$$

e aplicar o algoritmo de Euclides.

6. Sejam a_0, a_1, \dots, a_n inteiros e $x = \frac{r}{s}$ um número racional (com $\text{mdc}(r, s) = 1$) tal que

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = 0$$

Mostrar que $s \mid a_n$ e $r \mid a_0$.

7. Mostrar que a sucessão r_k de restos obtida pelo algoritmo de Euclides aplicado a inteiros $a > b > 0$ satisfaz $r_{k+2} < \frac{r_k}{2}$ e que portanto o número de passos necessário para o algoritmo terminar é majorado por $2 \log_2(b)$.

Definição 1.17 Dizemos que a e b são **primos entre si** se $\text{mdc}(a, b) = 1$.

Deduz-se portanto do resultado anterior que a e b são primos entre si se e só se existem inteiros x e y tais que

$$xa + yb = 1$$

Teorema 1.18 *Se $a, b, c \in \mathbb{Z}$,*

$$\text{mdc}(a, c) = 1 \text{ e } c \mid ab \implies c \mid b.$$

Demonstração 1.19 *De facto, como existem inteiros x, y tais que $ax + cy = 1$, temos*

$$abx + cby = b$$

e como c divide as duas parcelas da esquerda tem também que dividir b .

Corolário 1.20 *Se a, b_1, b_2, \dots, b_n são inteiros tais que*

$$\text{mdc}(a, b_i) = 1 \quad \forall i$$

então $\text{mdc}(a, b) = 1$, onde $b = \prod_{i=1}^n b_i$.

Demonstração 1.21 *Existem inteiros x_i e y_i (com $1 \leq i \leq n$) tais que*

$$ax_i + b_i y_i = 1 \quad \forall i$$

Multiplicando estas igualdades termo a termo obtemos

$$aX + bY = 1$$

onde $Y = y_1 y_2 \cdots y_n$.

Proposição 1.22 Se $\text{mdc}(a, b) = 1$

$$a|c \text{ e } b|c \implies (ab)|c$$

Demonstração 1.23 Sabemos que existem inteiros u, v tais que $au + bv = 1$; por outro lado, $c = ax = by$. Então,

$$c = acu + bcv = ab(uy + vx).$$

Mais geralmente,

Proposição 1.24 Se a_1, a_2, \dots, a_k são primos dois a dois, ou seja

$$\text{mdc}(a_i, a_j) = 1 \quad \forall i \neq j$$

então

$$a_i|c \quad \forall 1 \leq i \leq k \implies \left(\prod_{i=1}^k a_i\right)|c$$

Demonstração 1.25 Usamos indução: o caso $k = 2$ é o da proposição anterior; suponhamos então que a implicação é verdadeira para $k - 1$; então dados inteiros a_1, a_2, \dots, a_k nas condições do enunciado, temos que os $k - 1$ inteiros a_1, a_2, \dots, a_{k-1} também satisfazem essas condições e portanto, pela hipótese de indução, $(a_1 a_2 \dots a_{k-1})|c$; mas os dois inteiros $a_1 a_2 \dots a_{k-1}$ e a_k são primos entre si e ambos dividem c ; estamos portanto nas condições do caso $k = 2$ e podemos concluir, pela proposição anterior, que

$$(a_1 \dots a_k)|c$$

Corolário 1.26 Se $d = \text{mdc}(a, b)$, a equação

$$ax + by = c$$

tem soluções $x, y \in \mathbb{Z}$ se e só se $d \mid c$.

Além disso, se (x_0, y_0) é uma solução desta equação, o conjunto de todas as soluções é constituído pelos pares de inteiros (x, y) da forma

$$x = x_0 + k\frac{b}{d} \quad ; \quad y = y_0 - k\frac{a}{d} \quad ; \quad k \in \mathbb{Z}.$$

Demonstração 1.27 A primeira parte do resultado é óbvia: se $d = as + bt$ e $c = dm$, então $c = a(ms) + b(mt)$; por outro lado, se $c = ax + by$, então $d \mid c$.

Dada uma solução $c = ax_0 + by_0$, é evidente que, para qualquer $k \in \mathbb{Z}$, se tem também

$$c = a\left(x_0 + k\frac{b}{d}\right) + b\left(y_0 - k\frac{a}{d}\right)$$

Suponhamos que $c = az + bw$; então

$$ax_0 + by_0 = az + bw \Leftrightarrow a(x_0 - z) = b(w - y_0) \Leftrightarrow \frac{a}{d}(x_0 - z) = \frac{b}{d}(w - y_0)$$

Mas, como se verifica imediatamente a partir da definição de máximo divisor comum, se $\text{mdc}(a, b) = d$ então $\text{mdc}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$; logo, se $\frac{a}{d}$ divide o produto $\frac{b}{d}(w - y_0)$, pelo Teorema anterior tem que dividir $w - y_0$, ou seja, existe um inteiro k tal que

$$w = y_0 + k\frac{a}{d}.$$

Substituindo na equação anterior,

$$\frac{a}{d}(x_0 - z) = \frac{b}{d}(w - y_0) = k\frac{ba}{dd}$$

e portanto

$$z = x_0 - k\frac{b}{d}$$

como queríamos provar.

O conceito de máximo divisor comum generaliza-se a mais de dois inteiros e prova-se (ver exercícios) que

$$\text{mdc}(a_1, a_2, \dots, a_n) = \text{mdc}(\text{mdc}(a_1, a_2, \dots, a_{n-1}), a_n)$$

e a partir desta igualdade conclui-se que se $d = \text{mdc}(a_1, a_2, \dots, a_n)$, então existem inteiros x_i tais que

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

e que um inteiro c tem uma representação desta forma se e só se $d \mid c$. Mas a caracterização dos possíveis coeficientes x_i é um problema muito mais complicado (ver Ficha complementar de problemas).

Exercícios II.3

1. Mostrar que, para inteiros positivos a e b , $\log_a(b)$ é racional, ou seja, $\log_a(b) = \frac{m}{n}$ com $m, n \in \mathbb{N}$, se e só se existir $c \in \mathbb{N}$ tal que

$$a = c^n \text{ e } b = c^m.$$

Sugestão: Representar a e b como produto de factores primos e recordar que podemos escolher m e n primos entre si.

2. Determinar o máximo divisor comum d de 843 e 312 e inteiros x, y tais que

$$d = 843x + 312y$$

com $0 < x < 100$.

3. Calcular $d = \text{mdc}(649, 1694)$ e determinar os pares de inteiros x e y que satisfazem as condições

$$1694x + 649y = d \quad \text{e} \quad 0 < x + y < 100.$$

4. Determinar quantos pares de inteiros x, y existem satisfazendo as condições

$$1694x + 649y = 66 \quad \text{e} \quad |x + y| < 100.$$

5. Mostrar que os coeficientes x_k e y_k obtidos pelo algoritmo de Euclides estendido satisfazem a condição

$$x_{k-1}y_k - x_k y_{k-1} = (-1)^k \quad \forall k \geq 0;$$

em particular, $\text{mdc}(x_k, y_k) = 1$ para todo o k .

6. Mostrar que se, como resultado do algoritmo de Euclides estendido aplicado a a e b , $d = ax_m + by_m$, então, prolongando por mais uma linha obtemos inteiros x_{m+1} e y_{m+1} e

$$|x_{m+1}| = \frac{b}{d}, \quad |y_{m+1}| = \frac{a}{d}.$$

1.3 Números primos e o Teorema Fundamental da Aritmética

Definição 1.28 Um inteiro $p > 1$ diz-se **primo** se os seus únicos divisores positivos são 1 e o próprio p .

Deduz-se facilmente que qualquer inteiro $n > 1$ é divisível por algum primo. Além disso, o último corolário da secção anterior tem como consequência a seguinte

Proposição 1.29 Dados $a_1, a_2, \dots, a_n \in \mathbb{Z}$ e p primo,

$$p \mid a_1 a_2 \dots a_n \implies \exists i : p \mid a_i.$$

Teorema 1.30 *O conjunto dos números primos é infinito.*

Demonstração 1.31 *Seja de facto p_1, p_2, \dots, p_m um qualquer conjunto finito de primos (por exemplo, os primeiros m primos); o número*

$$N = p_1 p_2 \cdots p_m + 1$$

ou é primo ou tem que ter um factor primo p ; se $p \in \{p_1, p_2, \dots, p_m\}$ então p dividiria o produto $p_1 p_2 \cdots p_m$ e então teria que dividir 1, o que é impossível. Em qualquer caso verificamos que N tem um factor primo diferente de qualquer um dos p_i .

Teorema 1.32 *Teorema Fundamental da Aritmética*

Para cada inteiro $n > 1$, existem primos p_1, p_2, \dots, p_r , tais que

$$n = p_1 p_2 \cdots p_r$$

e essa factorização é única a menos de permutação dos factores.

Demonstração 1.33 *A demonstração deste Teorema pode ser feita por uma aplicação do Princípio de Indução Finita (Forte) e das propriedades deduzidas anteriormente:*

$n = 1$ é o produto do conjunto vazio de primos (tal como a soma de um conjunto vazio de números é igual a zero...) e $n = 2$ é primo; dado $n > 2$, suponhamos, como hipótese de indução, que todo o natural menor que n tem uma factorização única em factores primos.

Se n é primo tem evidentemente uma factorização única; caso contrário, podemos factorizar $n = n_1 n_2$ com $1 < n_1, n_2 < n$; por hipótese de indução, n_1 e n_2 têm ambas factorização única

$$n_1 = p_1 p_2 \cdots p_m, \quad n_2 = p'_1 p'_2 \cdots p'_l$$

e portanto n tem claramente uma factorização em factores primos

$$n = p_1 p_2 \cdots p_m p'_1 p'_2 \cdots p'_l$$

Para vermos que essa factorização é única notamos que se

$$n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$$

são duas factorizações em factores primos, então p_1 , por ser primo, divide forçosamente um dos factores q_i , que podemos supor, renumerando os factores, ser q_1 ; mas como este é primo, os seus únicos divisores (positivos) são 1 e q_1 e portanto $p_1 = q_1$.

Cancelando esse factor obtemos

$$\frac{n}{p_1} = p_2 \cdots p_s = q_2 \cdots q_t$$

e como $\frac{n}{p_1}$ é menor que n , tem factorização única em factores primos, ou seja $s = t$ e os q_i coincidem com os p_i , a menos de uma permutação dos factores. Mas então o mesmo acontece com as factorizações de n .

Se designarmos por p_k a sucessão crescente de todos os números primos, $p_1 = 2, p_2 = 3, \dots$, podemos escrever a factorização de n como

$$n = \prod_{k \geq 1} p_k^{i_k}$$

onde os expoentes i_k satisfazem a condição de serem 0 excepto para um número finito de casos, com a convenção de que o produto de um número infinito de 1 é 1 (à semelhança do que se passa com a soma de um número infinito de termos iguais a zero). Qualquer sucessão i_k que satisfaça as condições

$$i_k \geq 0 \forall k \geq 1, \quad \exists m : i_k = 0 \forall k > m$$

corresponde a uma factorização de um natural positivo e temos portanto uma bijecção entre o conjunto dos naturais positivos e o conjunto das sucessões

que satisfazem aquelas condições, e o produto de dois naturais corresponde, por essa bijecção, à soma das sucessões respectivas: se

$$n = \prod_{k \geq 1} p_k^{i_k}, \quad m = \prod_{k \geq 1} p_k^{j_k}$$

então

$$nm = \prod_{k \geq 1} p_k^{i_k + j_k}$$

A relação de divisibilidade $n \mid m$ traduz-se em $i_k \leq j_k, \forall k$ e, do mesmo modo,

$$\text{mdc}(n, m) = \prod_{k \geq 1} p_k^{\min\{i_k, j_k\}}, \quad \text{mmc}(n, m) = \prod_{k \geq 1} p_k^{\max\{i_k, j_k\}}$$

onde $\text{mmc}(n, m)$ designa o menor múltiplo comum dos dois naturais n e m .

Exercícios II.4

1. Se $\text{mdc}(a, b) = p$ e p é primo, quais são os possíveis valores de $\text{mdc}(a^2, b^3)$?
2. Dada a sucessão definida por

$$A_1 = 2 \wedge A_{n+1} = A_n^2 - A_n + 1, \forall n,$$

mostrar que $\text{mdc}(A_i, A_j) = 1$ para quaisquer $i \neq j$.

Sugestão: provar que $\forall n \ A_{n+1} = A_1 A_2 \cdots A_n + 1$.

3. Com quantos zeros termina a expansão decimal de $100!$?
Sugestão: dado um primo p , quantos inteiros $1 \leq n \leq 100$ são divisíveis por p ? e, para cada $k > 0$, quantos são divisíveis por p^k ? Deduzir uma fórmula para o maior inteiro m que satisfaz $p^m \mid n!$.
4. Dado um polinómio $f(x)$ com coeficientes inteiros e grau $t > 0$, mostrar que o conjunto dos primos que dividem $f(n)$ para algum inteiro n é infinito.
Sugestão: Começar por notar que basta considerar o caso $f(0) \neq 0$. Generalizar a demonstração de Euclides sobre a infinitude do conjunto

dos primos: supondo que $\{p_1, p_2, \dots, p_k\}$ é um conjunto finito de primos que dividem algum valor inteiro de f , e que contém os primos que dividem $f(0)$, e designando $P = \prod_{i=1}^k p_i$, considerar o inteiro $f(f(0)P)$.

5. Resolver os exercícios II.2.2. e II.2.4. usando o Teorema Fundamental da Aritmética.

6. Mostrar que se $n > 4$ não é primo então $n \mid (n - 1)!$.

7. Uma **tripla pitagórica** (x, y, z) é um triplo de naturais tais que $x^2 + y^2 = z^2$.

Uma tripla pitagórica diz-se primitiva se os três naturais não tiverem factor comum.

a) Mostrar que se $n > m > 0$ são naturais primos entre si em que um é par e o outro é ímpar, então $(n^2 - m^2, 2mn, n^2 + m^2)$ é uma tripla pitagórica primitiva.

b) Mostrar que se (x, y, z) é uma tripla pitagórica primitiva, então um de entre x e y é par e o outro, bem como z , é ímpar.

c) Suponhamos que $y = 2k$ é o termo par; deduzir que

$$k^2 = \frac{z - x}{2} \frac{z + x}{2}$$

e que os factores do lado direito são inteiros primos entre si.

d) Deduzir que cada um daqueles dois factores é um quadrado perfeito e concluir que todas as triplas pitagóricas primitivas (a menos de uma troca entre x e y) são da forma dada na alínea a).

Nota 1.34 *O Teorema Fundamental da Aritmética pode parecer evidente, de tal modo as propriedades dos números inteiros estão enraizadas na nossa mente. O seu alcance, e a sua dependência da validade do Lema da Divisão, são melhor compreendidos se estudarmos*

a aritmética de outros conjuntos. Para isso é conveniente reformular alguns dos conceitos apresentados de forma ligeiramente diferente.

Designemos por **unidades** de \mathbb{Z} os inteiros invertíveis, ou seja aqueles inteiros x para os quais existe algum inteiro y tal que $xy = 1$. Obviamente, as únicas unidades de \mathbb{Z} são 1 e -1 . Podemos então definir **número indecomponível** da seguinte forma: $x \neq 0$ é indecomponível se $x = yz$ implica que ou y ou z seja unidade.

É claro que em \mathbb{Z} um número é indecomponível exactamente se for primo ou o simétrico de um primo (ou se for ± 1), e como deduzimos atrás, esses inteiros podem também ser caracterizados pela propriedade

$$p \text{ é indecomponível} \Leftrightarrow (p \mid ab \implies p \mid a \vee p \mid b).$$

donde se seguem todos os resultados já deduzidos sobre os inteiros, incluindo o Teorema Fundamental da Aritmética.

Mas consideremos agora um outro exemplo de conjunto de números,

$$C = \{a + b\sqrt{10} \mid a, b \in \mathbb{Z}\}.$$

As operações de soma e multiplicação estão bem definidas neste conjunto, isto é, a soma e produto de dois números de C pertence ainda a C , e têm as mesmas propriedades elementares já descritas para \mathbb{Z} . Em particular, podemos definir a relação de divisibilidade e definir unidade e número indecomponível da mesma forma que fizemos para \mathbb{Z} . Note-se que C tem muito mais unidades do que \mathbb{Z} , por exemplo $3 + \sqrt{10}$ é unidade, com inverso $-3 + \sqrt{10}$, e portanto também $(3 + \sqrt{10})^k$ é unidade, para qualquer $k \geq 1$. Temos

$$2 \times 3 = (2 + \sqrt{10})(-2 + \sqrt{10}),$$

como se verifica facilmente. Mas, como se pode também verificar (embora menos facilmente) directamente a partir das definições, todos os números $2, 3, 2 + \sqrt{10}, -2 + \sqrt{10}$ são indecomponíveis. Portanto em C não vale o Teorema Fundamental da Aritmética, e um número indecomponível pode dividir o produto de dois números sem dividir nenhum deles.