Introdução à Teoria dos Números
Ficha 2: Aritmética de $\mathbb{Z}$

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

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

Como consequência do Princípio da Boa Ordenação de $\mathbb{N}$ (ver Ficha 1) temos

Lema 0.1 *da Divisão (inteira):*

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

$$a = bq + r \qquad e \qquad 0 \leq r < b.$$

Este Lema implica, por sua vez, o

Teorema 0.2 *(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*

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

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

Notação 0.3 *Escreve-se então $a = (r_n r_{n-1} \ldots r_2 r_1 r_0)_b$.*

Exercício 0.4 *Calcular a representação de* 29674 *na base* 3 *e na base* 11*.*

Definição 0.5 *Dados $a, b \in \mathbb{Z}$, não ambos nulos, diz-se que d é o* ***máximo divisor comum*** *de a e b, $d = mdc(a, b)$, 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 0.6 *Temos obviamente*

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

Teorema 0.7 *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 $v = 0$, $u = mdc(a, b)$.

Calculamos o Máximo Divisor Comum de $a = 5324$ e $b = 1023$; designamos os sucessivos restos obtidos por r_i, sendo $r_{-1} = a$ e $r_0 = b$.

Exemplo 0.8 *seja* $a = r_{-1} = 5324$ *e* $b = r_0 = 1023$*; obtemos sucessivamente*

$$\begin{aligned}
r_{-1} = 5324 = &\quad 5 \times 1023 + 209 = &\quad q_1 r_0 + r_1 \\
r_0 = 1023 = &\quad 4 \times 209 + 187 = &\quad q_2 r_1 + r_2 \\
r_1 = 209 = &\quad 1 \times 187 + 22 = &\quad q_3 r_2 + r_3 \\
r_2 = 187 = &\quad 8 \times 22 + 11 = &\quad q_4 r_3 + r_4 \\
r_3 = 22 = &\quad 2 \times 11 + 0 = &\quad q_5 r_4 + r_5
\end{aligned}$$

Conclui-se que $mdc(5324, 1023) = 11$.