Introdução à Teoria dos Números

Ficha 3: do algoritmo de Euclides ao Teorema Fundamental da Aritmética

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

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

Exercício 0.1 *Mostrar que para a, b positivos se tem*

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

Exercício 0.2 *Sejam $a_0, a_1, \cdots, a_n$ inteiros e $x = \frac{r}{s}$ um número racional (com $mdc(r, s) = 1$) tal que*

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

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

Definição 0.3 *Dizemos que a e b são **primos entre si** se $mdc(a, b) = 1$, ou seja, a e b são primos entre si se e só se existem inteiros x e y tais que*

$$xa + yb = 1$$

.

Se $a, b, c \in \mathbb{Z}$, e a e c são primos entre si, então existem inteiros x, y tais que

$$abx + cby = b,$$

e portanto $c \mid b$.

Se $mdc(a,b) = 1$

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

De facto, sabemos que existem inteiros u, v, x, y tais que $au + bv = 1$ e $c = ax = by$. Portanto,

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

Mais geralmente,

Se $a_1, a_2, \cdots, a_k$ são primos dois a dois, ou seja

$$mdc(a_i, a_j) = 1 \qquad \forall\, i \neq j$$

então

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

Exercício 0.4 *Demonstrar este resultado por indução.*

Se $d = mdc\,(a,b)$, 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

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

Exercício 0.5 *Deduzir (ou estudar nas Notas) a demonstração.*

Exercício 0.6 *Determinar o máximo divisor comum d de* 843 *e* 312 *e inteiros* x, y *tais que*

$$d = 843x + 312y$$

com $0 < x < 100$.

Definição 0.7 *Um inteiro* $p > 1$ *diz-se* ***primo*** *se os seus únicos divisores positivos são* 1 *e o próprio* p.

Os números primos caracterizam-se pela propriedade de dados $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ e p primo,

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

O conjunto dos números primos é infinito: Se $p_1, p_2, \cdots, p_m$ um qualquer conjunto finito de primos, os factores primos do número

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

são diferentes dos p_i.

Teorema 0.8 *Teorema Fundamental da Aritmética*

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

$$n = p_1 p_2 \ldots p_r$$

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