Aritmética dos Inteiros: o Lema da Divisão

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

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

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. $a \mid b \Leftrightarrow |a| \mid |b|$

Lema da Divisão (inteira)

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

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

Teorema

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

Máximo Divisor Comum

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 $c \mid b \implies c \mid d$.

Teorema

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

Algoritmo de Euclides para $mdc(a, b)$:

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

Exemplo

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

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

Máximo Divisor Comum

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

$$xa + yb = d.$$

$mdc(a, b)$ é o menor inteiro positivo que se pode escrever como combinação inteira de a e b.

Algoritmo de Euclides (estendido)

$$
\begin{array}{rrcr||r|r|r|r}
 & & & & r_i & q_i & x_i & y_i \\
 & & & & 2163 & & 1 & 0 \\
 & & & & 910 & & 0 & 1 \\
2163 = & 2 \times 910 & + & 343 & 343 & 2 & 1 & -2 \\
910 = & 2 \times 343 & + & 224 & 224 & 2 & -2 & 5 \\
343 = & 1 \times 224 & + & 119 & 119 & 1 & 3 & -7 \\
224 = & 1 \times 119 & + & 105 & 105 & 1 & -5 & 12 \\
119 = & 1 \times 105 & + & 14 & 14 & 1 & 8 & -19 \\
105 = & 7 \times 14 & + & 7 & 7 & 7 & -61 & 145 \\
14 = & 2 \times 7 & + & 0 & & & &
\end{array}
$$

E deduzimos que $mdc(2163, 910) = 7 = -61 \times 2163 + 145 \times 910$

Inteiros co-primos

Dois inteiros $a, b \in \mathbb{Z}$ dizem-se co-primos (ou primos entre si) se $mdc(a, b) = 1$, ou seja, se existem $x, y \in \mathbb{Z}$:

$$ax + by = 1$$

Consequências:

- $mdc\,(a, c) = 1$ e $c \mid ab \implies c \mid b$.
- Se $a, b_1, b_2, \cdots, b_n$ são inteiros tais que $mdc(a, b_i) = 1\ \forall i$, então $mdc(a, b) = 1$, onde $b = \prod_{i=1}^{n} b_i$
- 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

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

A equação $ax + by = c$

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

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

Números Primos

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

Dados $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ e p primo,

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

Teorema

O conjunto dos números primos é infinito.

Teorema Fundamental da Aritmética

Teorema

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.

Se

$$n = \prod_{k \geq 1} P_k^{i_k}, \qquad m = \prod_{k \geq 1} P_k^{j_k}$$

então

$$nm = \prod_{k \geq 1} P_k^{i_k + j_k}, \qquad mdc(n, m) = \prod_{k \geq 1} P_k^{\min\{i_k, j_k\}}$$