11. Algoritmo de Euclides

Sejam a e b dois números naturais, não ambos nulos. O algoritmo de Euclides permite calcular o máximo divisor comum d dos naturais a e b. Permite ainda encontrar dois inteiros s e t tais que

$$d = sa + tb.$$

Descrição do algoritmo: Calcular sucessivamente a divisão inteira dos pares (a, b), (b, r_0), (r_0, r_1), (r_1, r_2), etc., até que o resto seja zero:

$$\begin{aligned} a &= q_0 b + r_0; \\ b &= q_1 r_0 + r_1; \\ r_0 &= q_2 r_1 + r_2; \\ r_1 &= q_3 r_2 + r_3; \\ r_2 &= q_4 r_3 + r_4; \\ r_3 &= q_5 r_4 + r_5; \\ &\dots \end{aligned}$$

Se r_k é o primeiro resto que é zero, o máximo divisor comum entre a e b é $d = r_{k-1}$. Para obter os inteiros s e t, podemos escrever

$$\begin{aligned} d &= r_{k-1} \\ &= r_{k-3} - q_{k-1} r_{k-2} \\ &= (r_{k-5} - q_{k-3} r_{k-4}) - q_{k-1}(r_{k-4} - q_{k-2} r_{k-3}) \\ &\dots \end{aligned}$$

até chegar aos valores de a e b.

Resolução de equações de congruência módulo um número primo. Se queremos encontrar um inteiro x tal que

$$mx \equiv_p 1,$$

com p primo e $1 \leq m < p$: basta aplicar o algoritmo de Euclides ao par (m, p) e descobrir os inteiros s e t tais que $sm + tp = 1$ (m e p são primos entre si, porque p é primo e $m < p$). Assim, temos $ms = 1 \mod p$. Logo o conjunto das soluções em $\mathbb{Z}$ é

$$\{x \in \mathbb{Z} : x \equiv_p s\}.$$

Se quisermos resolver a equação

$$mx \equiv_p n,$$

com p primo e $1 \leq n, m < p$, podemos proceder da seguinte maneira: encontramos um inteiro y tal que $my = 1 \mod p$. Uma solução será $x = ny$. Logo, o conjunto das soluções em $\mathbb{Z}$ será

$$\{x \in \mathbb{Z} : x \equiv_p ny\}.$$

1. Determine o máximo divisor comum dos seguintes pares de inteiros (aplicando o método que entender):
   (a) $(20, 32)$;
   (b) $(20, 10)$;
   (c) $(20, 20)$;
   (d) $(20, -20)$;
   (e) $(-20, -20)$;
   (f) $(20, 1)$;
   (g) $(20, 0)$;
   (h) $(20, 72)$;
   (i) $(20, -72)$;
   (j) $(120, -72)$;
   (k) $(120, 162)$;
   (l) $(20, 27)$;
   (m) $(1234, 1235)$;
   (n) $(17, 34)$;
   (o) $(17, 72)$;
   (p) $(17, 850)$;
   (q) $(170, 850)$;
   (r) $(289, 850)$;
   (s) $(2890, 850)$.
2. Aplique o algoritmo de Euclides para encontrar o máximo divisor comum entre os seguintes pares de inteiros e para escrevê-lo na forma $d = sa + tb$, onde d, com $d = \text{mdc}(a, b)$.
   (a) $(20, 14)$;
   (b) $(14, 20)$;
   (c) $(20, 7)$;
   (d) $(20, 30)$;
   (e) $(72, 17)$;

(f) $(320, 30)$;

(g) $(289, 850)$;

(h) $(2890, 850)$;

(i) $(14259, 3521)$;

(j) $(8359, 9373)$.

3. Mostre que se d é o máximo divisor comum do par (a, b), então d é o menor inteiro positivo que se pode escrever na forma

$$d = sa + tb,$$

com s e t inteiros. [Sugestão: suponha que d é o máximo divisor comum do par (a, b) e considere um número inteiro positivo e tal que $e = sa + tb$; mostre que nesse caso, d divide e.]

4. Utilize o algoritmo de Euclides para encontrar o máximo divisor de cada um dos pares $(1597, 987)$ e $(1589, 997)$. Reconhece os números do primeiro par? Tente encontrar uma razão para que o algorimto termine mais cedo num caso do que no outro.

5. Resolva as seguintes equações em $\mathbb{Z}$ (no caso de serem impossíveis, explique porquê):

(a) $8x \equiv_{13} 1$;

(b) $8x \equiv_{13} 4$;

(c) $99x \equiv_{13} 1$;

(d) $99x \equiv_{13} 5$;

(e) $5x \equiv_{26} 1$;

(f) $11x \equiv_{26} 1$;

(g) $4x \equiv_{26} 1$;

(h) $9x \equiv_{26} 1$;

(i) $17x \equiv_{26} 1$;

(j) $13x \equiv_{26} 1$;

(k) $2000x \equiv_{643} 1$;

(l) $643x \equiv_{2000} 1$;

(m) $1647x \equiv_{788} 1$;

(n) $788x \equiv_{1647} 24$.

6. **Teorema chinês do resto.** Dados inteiros positivos $n_1, \ldots, n_k$, primos entre si dois a dois, e inteiros quaisquer $a_1, \ldots, a_k$, o sistema

$$\begin{cases} x \equiv_{n_1} a_1 \\ x \equiv_{n_2} a_2 \\ \quad \cdots \\ x \equiv_{n_k} a_k \end{cases}$$

é sempre possível. Mais, as suas soluções são todas congruentes módulo $N = n_1 \cdots n_k$.

Resolva os seguintes sistemas:

(a) $\begin{cases} x \equiv_{13} 8 \\ x \equiv_{99} 0 \end{cases}$;

(b) $\begin{cases} x \equiv_{13} 0 \\ x \equiv_{99} 65 \end{cases}$;

(c) $\begin{cases} x \equiv_{13} 0 \\ x \equiv_{11} 5 \\ x \equiv_{7} 4 \end{cases}$;

(d) $\begin{cases} x \equiv_{13} 1 \\ x \equiv_{11} 2 \\ x \equiv_{7} 3 \end{cases}$;

(e) $\begin{cases} x \equiv_{13} 3 \\ x \equiv_{11} 2 \\ x \equiv_{7} 1 \end{cases}$;

(f) $\begin{cases} x \equiv_{26} 5 \\ x \equiv_{21} 7 \\ x \equiv_{25} 4 \end{cases}$;

(g) $\begin{cases} x \equiv_{7} 2 \\ x \equiv_{8} 3 \\ x \equiv_{9} 5 \end{cases}$.