Máximo divisor comum

Quando se estuda o máximo divisor comum é frequentemente conveniente saber o seguinte teorema, cuja primeira parte é conhecida como *Lema de Bézout*.

Teorema. *Sejam a, b, c inteiros não nulos. Então a equação Diofantina $ax + by = c$ tem soluções se e só se c é um múltiplo de $mdc(a, b)$. Se x_0, y_0 é uma solução particular desta equação, então, fazendo $d = mdc(a, b)$, todas as outras soluções são dadas por*

$$x = x_0 + \left(\frac{b}{d}\right)t, \qquad y = y_0 - \left(\frac{a}{d}\right)t$$

onde t é um inteiro arbitrário.

A determinação de uma solução particular x_0, y_0 na equação anterior pode fazer-se usando o *Algoritmo de Euclides*, que é ensinado no Ensino Básico.

Étienne Bézout (1730-1783)

1. Um cliente comprou uma dúzia de peças de fruta — maçãs e laranjas — por 1,32 euros. Se uma maçã custa três cêntimos a mais do que uma laranja e se foram compradas mais maçãs do que laranjas, quantas peças de cada tipo de fruta foram compradas?

2. Se um galo vale 5 moedas, uma galinha vale 3 moedas, e três pintainhos juntos valem 1 moeda, quantos galos, galinhas e pintainhos, totalizando 100, podemos comprar com 100 moedas?

3. Dado um inteiro positivo n, seja $F_n = 2^{2^n} + 1$ (os números desta forma são os *números de Fermat*).

   (a) Mostrem que
   $$F_n - 2 = \prod_{k=0}^{n-1} F_k$$

   (b) Mostrem que se $m \neq n$, então F_m e F_n são primos entre si.

4. Os números naturais a e b são tais que
$$\frac{a+1}{b}+\frac{b+1}{a}$$
é um inteiro. Mostrem que o máximo divisor comum de a e b não é maior do que $\sqrt{a+b}$.

5. Provem que se u, a, b são inteiros positivos tais que $u \geq 2$, então
$$mdc(u^a-1, u^b-1) = u^{mdc(a,b)}-1$$

6. Determinem todos os inteiros k para os quais existe uma função $f\colon \mathbb{N} \to \mathbb{Z}$ tal que
   (a) $f(1997) = 1998$
   (b) $f(ab) = f(a)+f(b)+kf(mdc(a,b))$ para quaisquer $a, b \in \mathbb{N}$.

O Lema de Bézout admite a seguinte generalização.

Teorema. *Sejam $a_1, a_2, ..., a_m$ inteiros positivos. Seja c um inteiro. Então existem inteiros $x_1, x_2, ..., x_m$ tais que*
$$\sum_{i=1}^{m} a_i x_i = c$$
se e só se c é um múltiplo de $mdc(a_1, a_2, ..., a_m)$.

Em particular, se $mdc(a_1, a_2, ..., a_m) = 1$, então a equação
$$a_1x_1 + a_2x_2 + \cdots + a_kx_k = c$$
tem soluções inteiras, qualquer que seja o inteiro c. O que acontece se exigirmos apenas soluções inteiras não negativas? Essa questão é abordada no seguinte problema.

7. Sejam $a_1, a_2, \ldots, a_k$ inteiros positivos tais que o seu máximo divisor comum é 1. O *número de Frobenius* $g(a_1, \ldots, a_k)$ é o maior número natural c tal que a equação
$$a_1x_1 + a_2x_2 + \cdots + a_kx_k = c$$
não tem soluções inteiras $x_1, \ldots, x_k$ todas **não negativas**.

   Sejam a, b números inteiros positivos primos entre si. Provem que $g(a, b) = ab - a - b$.

   Este problema é conhecido como sendo o problema da moeda*, porque a sua solução resolve a seguinte questão: com moedas de valores inteiros a e b primos entre si, qual é maior quantia inteira que não pode ser paga apenas com moedas de valor a e b?*