Lista 7

Sejam a, b, n inteiros positivos e $d = \text{mdc}(a, n)$. Suponha que d divida b, e sejam

$$a' = \frac{a}{d}, \qquad b' = \frac{b}{d}, \qquad \text{e} \qquad n' = \frac{n}{d}.$$

Sabemos que a congruência linear

$$a'x \equiv b' \pmod{n'}$$

possui solução única *módulo* n', dada por

$$x \equiv \alpha b' \pmod{n'},$$

onde α é o inverso de a' módulo n', i.e., α é o coeficiente de a' em qualquer identidade de Bézout

$$\alpha a' + \beta n' = \text{mdc}(a', n') = 1.$$

Exercício 1.
Mostre que, para qualquer $r \in \mathbb{Z}$, temos que

$$x \equiv \alpha b' + rn' \pmod{n}$$

é uma solução da congruência

$$ax \equiv b \pmod{n}$$

Exercício 2.
Mostre que, para quaisquer $r, r' \in \mathbb{Z}$, temos

$$rn' \equiv r'n' \pmod{n} \qquad \text{se, e somente se} \qquad r \equiv r' \pmod{d}.$$

Exercício 3.
Usando os Exercícios 1 & 2, conclua que a congruência $ax \equiv b \pmod{n}$ possui exatamente $\text{mdc}(a, n)$ soluções módulo n.

Exercício 4.
Exercício 3 da página 130 do livro-texto.

Exercício 5.
Exercício 5 da página 130 do livro-texto.