Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte
Introdução à Teoria dos Números
Atividade em Dupla

Prof. Francisco Medeiros

Considere a equação modular

$$aX \equiv b \mod m, \tag{1}$$

onde $a, b, m \in \mathbb{Z}$, com $a \neq 0$ e $m > 1$. Denote por d o $\text{mdc}(a, m)$.

1. Seja $x \in \mathbb{Z}$. Mostre que (a) $\Rightarrow$ (b) $\Rightarrow$ (c) :
   (a) x é solução da equação (1).
   (b) $d \mid (ax - b)$.
   (c) $d \mid b$.
2. Tendo em vista o item anterior, determine uma condição necessária sobre os inteiros b e d para que a equação (1) admita solução em $\mathbb{Z}$. (Ficará claro no processo de resolução a seguir que essa condição também é suficiente.)
3. Escrevendo $a = a_1 d$ e $m = nd$, onde $a_1, n \in \mathbb{Z}$ e supondo que existe um inteiro b_1 de modo que $b = b_1 d$, temos assim que a equação (1) assume a forma seguinte

$$(a_1 d)X \equiv b_1 d \mod nd. \tag{2}$$

   (a) Verifique que os conjuntos solução de (2) e de

$$a_1 X \equiv b_1 \mod n \tag{3}$$

   são iguais.
   (b) Escrevendo $d = ra + sm$, mostre que $1 = ra_1 + sn$ e conclua que $ra_1 \equiv 1 \bmod n$.
   (c) Multiplique a equação (3) por r e use o item anterior para concluir que toda solução de (3) também é solução de

$$X \equiv rb_1 \mod n. \tag{4}$$

   (d) Seja agora x uma solução de (4). Verifique que $(ra_1)x \equiv rb_1 \bmod n$ e use o fato de $\text{mdc}(r, n) = 1$ (por quê?) para concluir que x também é solução de (3), ou seja, vale a congruência $a_1 x \equiv b_1 \bmod n$.
4. Conclua que os conjuntos solução de (1) e de (4) são iguais.
5. Encontre a solução geral de (4), e coloque-a em função dos inteiros r, b_1, m e d.