UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO
Departamento de Matemática Pura e Aplicada
Centro de Ciências Exatas, Naturais e da Saúde - CCENS

**Disciplina:** ***Álgebra I*** **Prof°.** ***Victor Martins***

# Lista 7: Congruências

(1) Seja $m$ um inteiro não nulo. Dados $a, b, c \in \mathbb{Z}$, mostre que se $ac \equiv bc(mod\, m)$ e $mdc(c, m) = d$, então $a \equiv b(mod\, \frac{m}{d})$.

(2) Sejam $a, b$ inteiros quaisquer, e sejam $m, d, r$ e $s$ inteiros positivos. Mostre que:

   (a) se $a \equiv b(mod\, m)$ e $d|m$, então $a \equiv b(mod\, d)$;
   (b) Se $a \equiv b(mod\, r)$ e $a \equiv b(mod\, s)$, então $a \equiv b(mod\, mmc(r, s))$;
   (c) se $ra \equiv rb(mod\, m)$, então $a \equiv b(mod\, \frac{m}{mdc(r,m)})$;
   (d) se $ra \equiv rb(mod\, rm)$, então $a \equiv b(mod\, m)$.

(3) Mostre que, se $[a]_m \in \mathbb{Z}_m$ for inversível, então seu inverso é único.

(4) Mostre que o produto de dois elementos inversíveis módulo $m$ é um elemento inversível.

(5) Mostre que se $[a]_m \cdot [c]_m = [b]_m \cdot [c]_m$ e $[c]_m$ for inversível, então $[a]_m = [b]_m$.

(6) Mostre que, se $p$ for um número primo, então todos os elementos não nulos de $\mathbb{Z}_p$ são inversíveis.

(7) Suponha que $a \equiv b(mod\, m)$ e $c \equiv d(mod\, m)$. Mostre que $ax + cy \equiv bx + dy(mod\, m)$ para quaisquer $x, y \in \mathbb{Z}$.

(8) Mostre que, se $a \equiv b(mod\, m)$, então $a^n \equiv b^n(mod\, m)$ para todo inteiro positivo $n$.

(9) Se $a = (72)^6 + (72)^5 + 2$, mostre que $7|a$.

(10) Demonstre o critério de divisibilidade por 11 usando congruências.

(11) Ache o resto da divisão de $a = 531 \cdot 2 \cdot (31)^2$ por 7.

(12) Resolva as congruênicas:

   (a) $3x \equiv 3(mod\, 5)$;
   (b) $3x \equiv 1(mod\, 6)$;
   (c) $3x \equiv 3(mod\, 6)$;

(13) Resolva a congruência $x^2 \equiv 4(mod\, 13)$.

(14) Mostre, por indução, que $4^n \equiv 1 + 3n (mod\, 9)$, se $n$ for um inteiro positivo.

(15) Ache o último algarismo dos números $9^{9^9}$ e $7^{7^7}$.

(16) Mostre que 8 é um número composto usando o Pequeno Teorema de Fermat.

(17) Mostre que 8 é um número composto utilizando o Teorema de Wilson.

(18) Verifique que $p = 341$ satisfaz o Pequeno Teorema de Fermat para $a = 2$, mas 341 não é um número primo.

(19) MOstre que 17 é um número primo utilizando o Teorema de Wilson.

(20) Mostre que 19 é um número primo utilizando o Teorema de Wilson.