

AUXILIAR 12

MATEMÁTICAS DISCRETAS

PROFESOR: PABLO BARCELÓ

AUXILIARES: ANTONIO LIZAMA & MIGUEL ROMERO

3 DE DICIEMBRE DE 2013

- P1.** Pruebe que si $a = b \pmod{m}$ entonces para todo $k \geq 1$, $a^k = b^k \pmod{m}$.
- P2.** Demuestre que si a y b son enteros positivos tal que $a > b$, entonces $(2^a - 1) \bmod (2^b - 1) = 2^{a \bmod b} - 1$.
- P3.** Pruebe que $\log 3$ es un número irracional.
- P4.** Pruebe que si $2^n - 1$ es un número primo, entonces n es primo.
- P5.** Pruebe que si p es primo, entonces cualquier solución de $x^2 = 1 \pmod{p}$ verifica

$$x = 1 \pmod{p} \quad \text{o} \quad x = -1 \pmod{p}$$

- P6.** Demostraremos la versión del pequeño teorema de Fermat que dice que si p es primo, y a es un entero cualquiera, entonces $a^p \equiv a \pmod{p}$. Para esto

- a) Demuestre que si $a \perp p$ (primos relativos), entonces no existen dos enteros congruentes $\pmod{p}$ en el conjunto $\{ja \mid j \in [1, \dots, p-1]\}$
- b) Demuestre que si $a \perp p$, entonces

$$(p-1)!a^{p-1} \equiv (p-1)! \pmod{p}$$

- c) Demuestre que si $a \perp p$, entonces

$$a^{p-1} \equiv 1 \pmod{p}$$

- d) Concluya que si a es cualquier entero, entonces

$$a^p \equiv a \pmod{p}$$