Universidad de la República - Facultad de Ingeniería - IMERL: Matemática Discreta 2

Primer parcial - 4 de mayo de 2015. Duración: 3 horas

N° de parcial	Cédula	Apellido y nombre	Salón	Teórico

Primera parte: Múltiple Opción

MO	
1	2

Ejercicio 1. Sea $0 \leq n < 99$ tal que $n \equiv 5^{2579} \pmod{99}$. Indicar cuál de las opciones es correcta:

A. $n = 56$. **B.** $n = 20$. **C.** $n = 86$. **D.** $n = 5$.

Ejercicio 2. Sea $0 \leq m < 297$ tal que $m \equiv 60^{181} \pmod{297}$. Indicar cuál de las opciones es correcta:

A. $m = 60$. **B.** $m = 27$. **C.** $m = 135$. **D.** $m = 81$.

Segunda parte: Desarrollo

Ejercicio 3. Sean $a, b, c \in \mathbb{Z}^+$, probar que:

a. $\operatorname{mcd}(a, b) = \text{mín}\{s > 0 : s = ax + by \text{ para algunos } x, y \in \mathbb{Z}\}$.

b. Si $\operatorname{mcd}(a, b) = 1$ y $a \mid bc$ entonces $a \mid c$.

(Cualquier resultado que utilicen en esta parte tienen que demostrarlo).

Ejercicio 4. Dado el sistema

$$\begin{cases} x \equiv 8 \pmod{56} \\ x \equiv 1 \pmod{21} \\ x \equiv 4 \pmod{36} \\ x \equiv 8 \pmod{49} \end{cases},$$

investigar si tiene solución, y en caso que tenga encontrar todas sus soluciones.

Ejercicio 5.

a. Sea p primo, probar que si $x^2 \equiv 1 \pmod{p}$ entonces $x \equiv 1 \pmod{p}$ o $x \equiv -1 \pmod{p}$.

b. Sea $n = pqr$ con p, q, r primos distintos. Probar que hay a lo sumo 8 soluciones módulo n a la ecuación $x^2 \equiv 1 \pmod{n}$.