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

PRIMER PARCIAL - 5 DE MAYO DE 2016. DURACIÓN: 3 HORAS

N° de parcial	Cédula	Apellido y nombre	Teórico

Ejercicio 1.

a. Calcular el inverso de 5 módulo 121.

b. Calcular el inverso de 5^4 módulo 121.

c. Calcular $15^{773} \pmod{121}$.

d. Calcular $15^{773} \pmod{5^4 \cdot 121}$

Ejercicio 2. Dado el sistema

$$\begin{cases} x & \equiv & 31 \pmod{56} \\ x & \equiv & 53 \pmod{105} \end{cases},$$

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

Ejercicio 3.

a. Dado $n > 1$ entero, probar que n es producto de primos sin utilizar el Teorema Fundamental de la Aritmética.

b. **i**) Probar que si $p > 2$ primo entonces es de la forma $4k \pm 1$ para algún $k \in \mathbb{Z}$.
ii) Probar que existen infinitos primos de la forma $4k - 1$.

Ejercicio 4. Sean $a \in \mathbb{Z}$ y $n \in \mathbb{N}$ tales que $\operatorname{mcd}(a, n) = 1$, definimos los conjuntos

$$A = \{0 \leq x < n\},$$

$$B = \{0 \leq x < n : \operatorname{mcd}(x, n) = 1\}.$$

Definimos $f : A \to A$ de la siguiente manera

$$f(x) = a \cdot x \text{ mód } n,$$

o sea $f(x)$ es el resto de la división entera de $a \cdot x$ entre n.

a. Probar que si $x \in B$ entonces $f(x) \in B$.

b. Probar que f define una biyección de B con B.

c. Probar que $a^{\#B} \equiv 1 \pmod{n}$.