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

EXAMEN - 11 DE JULIO DE 2017. DURACIÓN: 3 HORAS Y MEDIA.

N° de examen	Cédula	Apellido y nombre

Ejercicio 1.

a. Enunciar y demostrar la Identidad de Bézout.

b. Deducir el Lema de Euclides.

c. Hallar todos los $x \in \mathbb{Z}$ que cumplan:

$$\begin{cases} 5x \equiv 1 & (\text{mód } 47) \\ x \equiv 21^{44} & (\text{mód } 19)\,. \end{cases}$$

Ejercicio 2.

a. Sea G un grupo y $g \in G$ un elemento de orden finito.

i) Probar que si $k \in \mathbb{Z}$ entonces

$$\mathrm{o}\left(g^k\right) = \frac{\mathrm{o}(g)}{\mathrm{mcd}(o(g), k)}\,.$$

ii) Deducir que $\mathrm{o}\left(g^k\right) = \mathrm{o}(g)$ si y sólo si $\mathrm{mcd}(k, \mathrm{o}(g)) = 1$.

b. Sabiendo que el grupo $U(p)$ de invertibles módulo un primo p es cíclico, probar que existen $\varphi(p-1)$ raíces primitivas módulo p.

Ejercicio 3.

a. i) Probar que 103 es un número primo.

ii) Probar que $g = 5$ es una raíz primitiva módulo el primo $p = 103$.

iii) Sabiendo que $g^{102} \equiv 1752 \pmod{103^2}$, probar que g es una raíz primitiva módulo p^2.

iv) Probar que g es una raíz primitiva módulo p^k para cada $k > 2$.

b. i) Describir el método de intercambio de claves de Diffie-Hellman.

ii) Mostrar que en el método Diffie-Hellman ambos participantes llegan a la misma clave.

Ejercicio 4.

a. Describir todos los elementos de $(U(15), \times)$ indicando su orden y cuál es su inverso.

b. Describir todos los homomorfismos de $(\mathbb{Z}_4, +)$ en $(U(15), \times)$.
Indicar cuáles son inyectivos.

c. i) Encontrar un homomorfismo inyectivo $f : (\mathbb{Z}_2, +) \to (U(15), \times)$ y un homomorfismo inyectivo $g : (\mathbb{Z}_4, +) \to (U(15), \times)$ tales que $\mathrm{Im}(f) \cap \mathrm{Im}(g) = \{1\}$.

ii) Probar que la función $h : (\mathbb{Z}_2 \times \mathbb{Z}_4, +) \to (U(15), \times)$ dada por

$$h(a, b) = f(a)\, g(b)$$

es un homomorfismo.

iii) ¿Es el homomorfismo h un isomorfismo?