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

EXAMEN - 20 DE DICIEMBRE DE 2017. DURACIÓN: 3 HORAS

N° de examen	Cédula	Apellido y nombre

Para cada pregunta o ejercicio, deben presentar claramente el razonamiento y cálculos realizados para obtener su respuesta final. Si una implicancia es válida debido a algún teorema, proposición o propiedad, deben especificarlo (nombre del teorema, lema, etc.) Presentar una respuesta final a la pregunta sin justificación carece de validez.

Ejercicio 1.

a. Definir la función φ de Euler.

b. Enunciar y demostrar el Teorema de Euler.

c. i) Probar que 127 es primo.
ii) Hallar $0 \leq x < 127$ tal que $x \equiv 3^{502} \pmod{127}$.

d. Hallar $0 \leq x < 363$ tal que $x \equiv 12^{332} \pmod{363}$.

Ejercicio 2.

a. Sea G un grupo abeliano y $x, y \in G$ tales que $\mathrm{o}(x) = ab$, con $a, b \in \mathbb{Z}^+$.

i) Probar que $\mathrm{o}(x^a) = b$. (OJO: si van a utilizar alguna fórmula para $o(x^k)$, deben probarla.)
ii) Probar que si x e y tienen órdenes coprimos entonces $\mathrm{o}(xy) = \mathrm{o}(x)\mathrm{o}(y)$.

b. Sea G el grupo de invertibles módulo 157, $G = U(157)$.

i) Sabiendo que en G, $\mathrm{o}(16) = 13$ y que $2^{12} \equiv 14 \pmod{157}$, hallar el orden de 2 en G.
ii) Sabiendo que $2^{46} \equiv 27 \pmod{157}$ hallar el orden de 3 en G.
iii) Hallar una raíz primitiva módulo 157.
iv) ¿Cuántos homomorfismos $f : U(314) \to \mathbb{Z}_{15}$ hay?

Ejercicio 3.

a. Hallar todos los pares (a, b) de enteros positivos tales que

$$a + b = 87 \quad \text{y} \quad \mathrm{mcd}(a, b) + \mathrm{mcm}(a, b) = 633.$$

b. Enunciar y demostrar el Lema de Euclides.

c. Hallar todos los pares (a, b) de enteros positivos tales que

$$ab + 3a = \frac{4b^2}{\mathrm{mcd}(a, b)} + 9b.$$