

Lunes 13 de Diciembre de 2010.

## EXAMEN DE MATEMÁTICA DISCRETA 2

Nombre .....	C.I. ....	No. de prueba .....
--------------	-----------	---------------------

**Ejercicio 1.** Se considera  $S_7$  el grupo de permutaciones de 7 elementos.

- (a) Exhiba un elemento de orden 5 y otro de orden 10.
- (b) Sean  $\gamma$  un  $k$ -ciclo y  $\sigma$  un  $l$ -ciclo disjuntos. Expresar el orden de  $\gamma\sigma$  en función de  $k$  y  $l$  y demostrar el resultado.
- (c) ¿Siguiendo siendo válida la expresión de la parte (b) si los ciclos no son disjuntos? Demuestre o muestre un contraejemplo.
- (d) Pruebe que no hay elementos de orden 14 en  $S_7$ .

**Ejercicio 2.** Sea  $n$  un entero,  $n \geq 2$ .

- (a) Probar que  $b^n \equiv b \pmod n$ ,  $\forall b \in \{1, \dots, n\}$  si y sólo si para todo  $p$  divisor primo de  $n$  se tiene que  $p^2 \nmid n$  y  $p-1 \mid n-1$ .
- (b) Sea  $n$  compuesto y en las condiciones de la parte (a).
  - (i) Probar que  $n$  es impar.
  - (ii) Probar que  $n$  posee al menos tres factores primos distintos.

**Ejercicio 3.**

- (a) Describa el método Diffie-Hellman para intercambio de clave.
- (b) ¿Es 7 raíz primitiva módulo 47? Justifique.
- (c) Con Fulano, para utilizar el método de Diffie-Hellman, se fija el primo  $p = 47$  y la base  $g = 7$ . Si usted elige el entero  $m = 44$  y recibe de Fulano el número 9, halle la clave  $c \in \{0, \dots, 46\}$ .