Álgebra (Ingeniería Informática) **Curso 2005-2006**

Práctica 3.2
(Teorema de Euler-Fermat)

1. Calcular el orden de cada uno de los elementos de: (a) $\mathbb{Z}_7^*$ (b) $\mathbb{Z}_6^*$.
2. Comprobar que tanto 3 como 6 son generadores de $\mathbb{Z}_7^*$. Decidir si 2 es también generador y razonar la respuesta.
3. Demostrar que si $3^\alpha \equiv 3^\beta \equiv 1 \pmod 7$ entonces también $3^{\mathrm{mcd}(\alpha,\beta)} \equiv 1 \pmod 7$.
4. Encontrar g tal que $\mathbb{Z}_{17}^* = \{g, g^2, g^3, \ldots, g^{16}\}$. (**Indicación:** Utilizar la demostración del Teorema 3.20).
5. Usar el Pequeño Teorema de Fermat para calcular:

   (a) $5^{2003} \pmod 7$ (b) $5^{2003} \pmod{11}$ (b) $5^{2003} \pmod{13}$.

6. Usar el ejercicio anterior y el Teorema Chino de los Restos para calcular $5^{2003} \pmod{1001}$. (**Indicación:** Observa que $1001 = 7 \cdot 11 \cdot 13$).
7. Sea $n \in \mathbb{N}$ y sea a coprimo con n. Se dice que a es un *residuo cuadrático* módulo n si la ecuación $x^2 \equiv a \pmod n$ tiene solución.
   (a) Encontrar los residuos cuadráticos módulo 11.
   (b) Demostrar que si $p \geq 3$ es primo y a no es divisible por p, entonces la ecuación $x^2 \equiv a \pmod p$ o bien no tiene soluciones, o bien tiene exactamente dos soluciones módulo p.
   (c) Demostrar que si $p \geq 3$ es primo entre los enteros $1, 2, \ldots, p-1$ hay exactamente $\frac{p-1}{2}$ residuos cuadráticos.
8. Encontrar todas las soluciones de la ecuación $x^2 \equiv 29 \pmod{35}$. (**Indicación:** Resuelve la congruencia módulo 5 y módulo 7 y utiliza el teorema chino del resto).
9. Demostrar que 2047 pasa el test de Miller-Rabin para la base 2, pero que es compuesto.