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

PRIMER PARCIAL - 25 DE ABRIL DE 2019.

Primera parte: Múltiple Opción

MO	
1	2
C.	**A.**

Ejercicio 1. Sea $0 \leq n < 104$ tal que $n \equiv 7^{4756} \pmod{104}$. Indicar cuál de las opciones es correcta:

A. $n = 25$. **B**. $n = 1$. **C**. $n = 9$. **D**. $n = 7$.

Solución: Como 7 y $104 = 2^2 \cdot 13$ son coprimos, podemos aplicar el Teorema de Euler. La función Euler en 104 es igual a $\varphi(104) = \varphi(2^2)\varphi(13) = 2 \cdot 12 = 48$, y $4756 \equiv 4 \pmod{104}$, entonces $n \equiv 7^4 \pmod{104} \equiv 2401 \pmod{104} \equiv 9 \pmod{104}$.

Ejercicio 2. Sea $0 \leq m < 272$ tal que $m \equiv 40^{241} \pmod{272}$. Indicar cuál de las opciones es correcta:

A. $m = 176$. **B**. $m = 40$. **C**. $m = 136$. **D**. $m = 160$.

Solución: Como 40 y $272 = 2^4 \cdot 17$ no son comprimos, no podemos aplicar Euler, por lo que aplicamos el Teorema Chino del Resto.

$$\begin{cases} m \equiv 40^{241} \pmod{2^4} \equiv 0 \pmod{2^4} \\ m \equiv 40^{241} \pmod{17} \equiv 6^{241} \pmod{17}. \end{cases}$$

Para la segunda congruencia aplicamos Euler, $\varphi(17) = 16$ y $241 \equiv 1 \pmod{16}$, por lo que $6^{241} \equiv 6 \pmod{17}$, y

$$\begin{cases} m \equiv 0 \pmod{16} \\ m \equiv 6 \pmod{17}. \end{cases}$$

Esto tiene solución $176 = 16 \cdot 11 = 17 \cdot 10 + 6$.

Segunda parte: Desarrollo

Ejercicio 3.

a. Sean $a, b, c \in \mathbb{Z}^+$.

i) Probar que $\operatorname{mcd}(a, b) = \min\{s > 0 : s = ax + by \text{ para algunos } x, y \in \mathbb{Z}\}$.
ii) Enunciar la Identidad de Bezout.
iii) Probar que $\operatorname{mcd}(ca, cb) = c \operatorname{mcd}(a, b)$.

(Cualquier resultado que utilicen en esta parte tienen que demostrarlo).
Solución: Ver las notas de teórico.

b. Hallar el inverso de 8 módulo 141 y el inverso de 16 módulo 141.
Solución: Aplicando el algoritmo extendido de Euclides encontramos que $8 \cdot 53 + 141 \cdot (-3) = 1$, por lo que $8^{-1} \equiv 53 \pmod{141}$. Por otro lado $16^{-1} \equiv 2^{-1}8^{-1} \pmod{141} \equiv 71 \cdot 53 \equiv 3763 \pmod{141} \equiv 97 \pmod{141}$

Ejercicio 4. Cierto producto se puede envasar en cajas de 50 o 52 unidades. Tenemos entre 1000 y 3000 unidades de ese producto. Sabemos que si las envasamos en cajas de 50 unidades nos quedan 27 afuera, y si las envasamos en cajas de 52 unidades nos faltan 3 para completar todas las cajas usadas.

a. Modelar lo anterior como un sistema de dos congruencias.
Solución: Si x es la cantidad de unidades que tenemos, el sistema de congruencias nos queda

$$\begin{cases} x \equiv 27 \pmod{50} \\ x \equiv -3 \pmod{52}, \end{cases}$$

con $1000 \leq x \leq 3000$.

b. Usando la parte **a**, responder cuántas unidades tenemos.
Solución: Resolver el sistema es equivalente a la diofántica

$$50k + 52k' = 30,$$

donde $x = 50k + 27$, $x = -52k' - 3$, que tiene solución porque $\text{mcd}(50, 52) = 2$ divide a 30. Una solución particular es $k = 15$, $k' = -15$, por lo que $k = 15 + 52/2 \cdot l = 15 + 26l$ para $l \in \mathbb{Z}$. Por lo tanto $x = 750 + 1300l + 27 = 777 + 1300l$ para algún $l \in \mathbb{Z}$. Como $1000 \leq x \leq 3000$, concluimos que $x = 777 + 1300 = 2077$.

Ejercicio 5. Demostrar que existen infinitos primos.
Solución: Ver notas teóricas.