

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

PRIMER PARCIAL - 4 DE MAYO DE 2015. DURACIÓN: 3 HORAS

**Ejercicio 1.** Sea  $0 \leq n < 99$  tal que  $n \equiv 5^{2579} \pmod{99}$ . Indicar cuál de las opciones es correcta:

- A.  $n = 56$ .                      B.  $n = 20$ .                      C.  $n = 86$ .                      D.  $n = 5$ .

Como 5 y 99 son coprimos podemos aplicar el teorema de Euler. Como  $99 = 3^2 \cdot 11$  entonces  $\varphi(99) = 2 \cdot 3 \cdot 10 = 60$ . También  $2579 \equiv -1 \pmod{60}$  y aplicando el teorema de Euler

$$5^{2579} \equiv 5^{-1} \pmod{99}.$$

Aplicando el Algoritmo Extendido de Euclides, el inverso de 5 módulo 99 es 20. Por lo tanto la solución es **20**.

**Ejercicio 2.** Sea  $0 \leq m < 297$  tal que  $m \equiv 60^{181} \pmod{297}$ . Indicar cuál de las opciones es correcta:

- A.  $m = 60$ .                      B.  $m = 27$ .                      C.  $m = 135$ .                      D.  $m = 81$ .

Como  $60 = 2^2 \cdot 3 \cdot 5$  no es coprimo con  $297 = 3^3 \cdot 11$  no podemos aplicar el teorema de Euler. Aplicando el Teorema Chino del Resto obtenemos

$$x \equiv 60^{181} \pmod{297} \Leftrightarrow \begin{cases} x \equiv 60^{181} \pmod{3^3} \\ x \equiv 60^{181} \pmod{11} \end{cases} \Leftrightarrow \begin{cases} x \equiv 3^{181} \cdot 20^{181} \pmod{3^3} \\ x \equiv 60^{181} \pmod{11} \end{cases}.$$

Ahora como  $3^3 \mid 3^{181}$  entonces  $60^{181} \equiv 0 \pmod{3^3}$ . Por otro lado  $\varphi(11) = 10$  y  $181 \equiv 1 \pmod{10}$ , por lo que  $60^{181} \equiv 60 \pmod{11} \equiv 5 \pmod{11}$ . Concluimos que

$$x \equiv 60^{181} \pmod{297} \Leftrightarrow \begin{cases} x \equiv 0 \pmod{3^3} \\ x \equiv 5 \pmod{11} \end{cases},$$

que tiene solución **27**.

## Segunda parte: Desarrollo

**Ejercicio 3.** Sean  $a, b, c \in \mathbb{Z}^+$ , probar que:

- a.  $\text{mcd}(a, b) = \min \{s > 0 : s = ax + by \text{ para algunos } x, y \in \mathbb{Z}\}.$

Ver notas de teórico.

- b. Si  $\text{mcd}(a, b) = 1$  y  $a \mid bc$  entonces  $a \mid c$ .

Ver notas de teórico.

(Cualquier resultado que utilicen en esta parte tienen que demostrarlo).

**Ejercicio 4.** Dado el sistema

$$\begin{cases} x \equiv 8 & (\text{mód } 56) \\ x \equiv 1 & (\text{mód } 21) \\ x \equiv 4 & (\text{mód } 36) \\ x \equiv 8 & (\text{mód } 49) \end{cases},$$

investigar si tiene solución, y en caso que tenga encontrar todas sus soluciones.

Como  $56 = 2^3 \cdot 7$ ,  $21 = 3 \cdot 7$ ,  $36 = 2^2 \cdot 3^2$  y  $49 = 7^2$ , entonces

$$x \equiv 8 \pmod{56} \Leftrightarrow \begin{cases} x \equiv 8 & (\text{mód } 8) \\ x \equiv 8 & (\text{mód } 7) \end{cases} \Leftrightarrow \begin{cases} x \equiv 0 & (\text{mód } 8) \\ x \equiv 1 & (\text{mód } 7) \end{cases}, \quad (1)$$

$$x \equiv 1 \pmod{21} \Leftrightarrow \begin{cases} x \equiv 1 & (\text{mód } 3) \\ x \equiv 1 & (\text{mód } 7) \end{cases} \Leftrightarrow \begin{cases} x \equiv 1 & (\text{mód } 3) \\ x \equiv 1 & (\text{mód } 7) \end{cases}, \quad (2)$$

$$x \equiv 4 \pmod{36} \Leftrightarrow \begin{cases} x \equiv 4 & (\text{mód } 4) \\ x \equiv 4 & (\text{mód } 9) \end{cases} \Leftrightarrow \begin{cases} x \equiv 0 & (\text{mód } 4) \\ x \equiv 4 & (\text{mód } 9) \end{cases}. \quad (3)$$

Como  $x \equiv 0 \pmod{8}$  implica  $x \equiv 0 \pmod{4}$ ,  $x \equiv 4 \pmod{9}$  implica  $x \equiv 4 \pmod{9}$  y  $x \equiv 8 \pmod{49}$  implica  $x \equiv 1 \pmod{7}$ , entonces el sistema original es **equivalente** a

$$\begin{cases} x \equiv 0 & (\text{mód } 8) \\ x \equiv 4 & (\text{mód } 9) \\ x \equiv 8 & (\text{mód } 49) \end{cases}$$

que tiene solución **400 módulo  $8 \cdot 9 \cdot 49 = 3528$** .

**Ejercicio 5.**

- a. Sea  $p$  primo, probar que si  $x^2 \equiv 1 \pmod{p}$  entonces  $x \equiv 1 \pmod{p}$  o  $x \equiv -1 \pmod{p}$ .

Si  $x^2 \equiv 1 \pmod{p}$  entonces  $0 \equiv (x^2 - 1) \pmod{p} \equiv (x - 1)(x + 1) \pmod{p}$  y  $p \mid (x - 1)(x + 1)$ .

Ahora, como  $p$  es primo  $p \mid (x - 1)$  o  $p \mid (x + 1)$ , por lo cual

$$x \equiv 1 \pmod{p} \text{ o } x \equiv -1 \pmod{p}.$$

Observar que ambas posibilidades son ciertas si y solo si  $p = 2$  ya que en ese caso  $1 \equiv -1 \pmod{p}$  que implica  $p \mid 2$ .

- b. Sea  $n = pqr$  con  $p, q, r$  primos distintos. Probar que hay a lo sumo 8 soluciones módulo  $n$  a la ecuación  $x^2 \equiv 1 \pmod{n}$ .

Si  $x^2 \equiv 1 \pmod{pqr}$  entonces  $x^2 \equiv 1 \pmod{p}$ ,  $x^2 \equiv 1 \pmod{q}$  y  $x^2 \equiv 1 \pmod{r}$ . Usando la parte anterior sabemos que

$$\begin{cases} x \equiv 1 & (\text{mód } p) \\ \text{o} \\ x \equiv -1 & (\text{mód } p) \end{cases} \text{ y } \begin{cases} x \equiv 1 & (\text{mód } q) \\ \text{o} \\ x \equiv -1 & (\text{mód } q) \end{cases} \text{ y } \begin{cases} x \equiv 1 & (\text{mód } r) \\ \text{o} \\ x \equiv -1 & (\text{mód } r) \end{cases}$$

por lo que

$$\begin{aligned}
& \left\{ \begin{array}{l} x \equiv 1 \pmod{p} \\ y \equiv 1 \pmod{q} \\ x \equiv 1 \pmod{r} \end{array} \right. \text{ o } \left\{ \begin{array}{l} x \equiv 1 \pmod{p} \\ y \equiv -1 \pmod{q} \\ x \equiv 1 \pmod{r} \end{array} \right. \text{ o } \left\{ \begin{array}{l} x \equiv 1 \pmod{p} \\ y \equiv -1 \pmod{q} \\ x \equiv -1 \pmod{r} \end{array} \right. \\
& \left\{ \begin{array}{l} x \equiv 1 \pmod{p} \\ y \equiv 1 \pmod{q} \\ x \equiv -1 \pmod{r} \end{array} \right. \text{ o } \left\{ \begin{array}{l} x \equiv -1 \pmod{p} \\ y \equiv 1 \pmod{q} \\ x \equiv 1 \pmod{r} \end{array} \right. \text{ o } \left\{ \begin{array}{l} x \equiv -1 \pmod{p} \\ y \equiv -1 \pmod{q} \\ x \equiv 1 \pmod{r} \end{array} \right. \text{ o } \\
& \left\{ \begin{array}{l} x \equiv -1 \pmod{p} \\ y \equiv 1 \pmod{q} \\ x \equiv -1 \pmod{r} \end{array} \right. \text{ o } \left\{ \begin{array}{l} x \equiv -1 \pmod{p} \\ y \equiv -1 \pmod{q} \\ x \equiv -1 \pmod{r} \end{array} \right. ,
\end{aligned}$$

que son las 8 opciones posibles.