

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

PRIMER PARCIAL - 30 DE SETIEMBRE DE 2015.  
Solución.

**Ejercicio 1.**

a. Enunciar el Teorema de Euler.

Ver notas teóricas: Teorema 2.6.5 en la página 40.

b. Calcular las siguientes potencias.

i)  $3^{100}$  (mód 104). Como  $104 = 2^3 \cdot 13$  entonces  $\varphi(104) = 2^2 \cdot 12 = 48$ . Para calcular la potencia podemos utilizar el teorema de Euler ya que 3 y 104 son coprimos, con lo que nos queda

$$3^{100} = 3^{48 \cdot 2 + 4} = (3^{48})^2 3^4 \equiv 3^4 \pmod{104} \equiv 81 \pmod{104}.$$

ii)  $10^{97}$  (mód 101). En este caso también podemos aplicar el teorema de Euler ya que 101 es primo. Como 101 es primo  $\varphi(101) = 100$  y  $10^{97} \equiv 10^{-3} \pmod{101} \equiv (10^{-1})^3 \pmod{101}$ .

Tenemos que calcular  $10^{-1} \pmod{101}$ , y para esto observamos que  $10 \cdot 10 = 100 \equiv -1 \pmod{101}$  entonces  $10 \cdot (-10) \equiv 1 \pmod{101}$  y concluimos que  $10^{-3} \equiv (-10)^3 \pmod{101} \equiv (-1000) \pmod{101} \equiv 10 \pmod{101}$ .

iii)  $6^{66}$  (mód 99).

En este caso no podemos aplicar el teorema de Euler dado que  $6 = 2 \cdot 3$  y  $99 = 3^2 \cdot 11$  no son coprimos. Lo que podemos hacer es aplicar el teorema chino del resto de la siguiente manera:

$$x \equiv 6^{66} \pmod{99} \Leftrightarrow \begin{cases} x \equiv 6^{66} \pmod{9} \\ x \equiv 6^{66} \pmod{11} \end{cases} \Leftrightarrow \begin{cases} x \equiv 0 \pmod{9} \\ x \equiv 6^6 \pmod{11} \end{cases}.$$

Calculamos  $6^6 \pmod{11}$  que es 5. La solución del sistema es 27 y entonces  $6^{66} \equiv 27 \pmod{101}$ .

*Aclaración: cuando pedimos calcular  $a^m \pmod{n}$ , nos referimos a hallar  $x \in \mathbb{N}$ , con  $0 \leq x < n$  tal que  $a^m \equiv x \pmod{n}$*

**Ejercicio 2.**

a. Sean  $a, b$  y  $c$  enteros no nulos tales que  $\text{mcd}(a, b) \mid c$ . Consideramos la ecuación diofántica

$$ax + by = c$$

y  $(x_0, y_0)$  una solución particular de la misma.

i) Probar que para todo  $k \in \mathbb{Z}$  el par

$$\left( x_0 + k \frac{b}{\text{mcd}(a, b)}, y_0 - k \frac{a}{\text{mcd}(a, b)} \right)$$

también es solución de la ecuación.

ii) Probar que todas las soluciones de la ecuación son de la forma

$$\left( x_0 + k \frac{b}{\text{mcd}(a, b)}, y_0 - k \frac{a}{\text{mcd}(a, b)} \right).$$

Es decir, probar que si  $(x_1, y_1)$  es solución de la ecuación, entonces existe  $k \in \mathbb{Z}$  tal que

$$(x_1, y_1) = \left( x_0 + k \frac{b}{\text{mcd}(a, b)}, y_0 - k \frac{a}{\text{mcd}(a, b)} \right).$$

La solución de ambas partes es el Teorema 1.5.3 de las notas teóricas en la página 17.

- b. i) Hallar todas las soluciones módulo 41 de la ecuación  $4x \equiv 7 \pmod{41}$ .

Como 4 es invertible módulo 41 hay una sola solución a la congruencia que será  $x \equiv 4^{-1} \cdot 7 \pmod{41}$ . Como  $4 \cdot 10 \equiv -1 \pmod{41}$  y  $4^{-1} \equiv -10 \pmod{41} \equiv 31$ . Por lo tanto  $x \equiv 7 \cdot -10 \pmod{41} \equiv -70 \pmod{41} \equiv 12 \pmod{41}$ .

- ii) Hallar todas las soluciones módulo 80 de la ecuación  $25x \equiv 10 \pmod{80}$ .

En este caso no podemos hacer lo mismo que en el caso anterior dado que 25 no es invertible módulo 80. Pero la congruencia anterior es equivalente a la diofántica

$$25x + 80y = 10,$$

que claramente tiene solución dado que  $\text{mcd}(25, 80) = 5 \mid 10$ . Una solución particular es  $(-6, 2)$  encontrada utilizando el Algoritmo Extendido de Euclides. Esto implica que todas las soluciones de  $x$  son de la forma

$$-6 + \frac{80}{5}k = -6 + 16k.$$

Y como nos interesa los  $x$  módulo 80 vemos que las soluciones son  $x \equiv -6 + 16k \pmod{80}$  con  $k = 0, 1, 2, 3, 4$ . Las calculamos y dan

$$x \equiv 10, 26, 42, 58, 74 \pmod{80}.$$

**Ejercicio 3.** Para cada uno de los siguientes sistemas, investigar si tiene solución, y en caso que tenga solución, hallar todas sus soluciones.

$$\text{a. } \begin{cases} x \equiv 7 \pmod{11} \\ x \equiv 13 \pmod{20} \\ x \equiv 14 \pmod{21} \end{cases} \quad \text{b. } \begin{cases} x \equiv 7 \pmod{22} \\ x \equiv 21 \pmod{28} \\ x \equiv 23 \pmod{30} \end{cases}.$$

- a. Dado que los módulos del sistema son coprimos 2 a 2 sabemos que el sistema tiene solución por el Teorema Chino del Resto. Utilizamos el método dado en el ejercicio 4 del práctico 5 para su resolución, pero antes aplicamos un cambio de variable lineal para facilitar las cuentas. Si definimos  $x' = x + 7$ , entonces el nuevo sistema a resolver es

$$\begin{cases} x' \equiv 3 \pmod{11} \\ x' \equiv 0 \pmod{20} \\ x' \equiv 0 \pmod{21} \end{cases}.$$

Ahora, la solución al sistema viene dada por  $x' \equiv 3b_1M_1 + 0b_2M_2 + 0b_3M_3 \pmod{11 \cdot 20 \cdot 21}$ , donde  $b_i$  es el inverso de  $M_i$  módulo  $m_i$ .  $m_i$  son los módulos y  $M_i$  es el producto de todos los módulos menos el  $i$ -ésimo. Entonces solo tenemos que calcular el inverso de  $M_1 = 20 \cdot 21$  módulo 11. Ahora  $20 \cdot 21 \equiv (-2) \cdot (-1) \pmod{11} \equiv 2 \pmod{11}$  y  $M_1^{-1} \equiv 6 \pmod{11}$ . Por lo tanto la solución al sistema con  $x'$  es  $3 \cdot 6 \cdot 20 \cdot 21 = 7560 \equiv 2940 \pmod{11 \cdot 20 \cdot 21}$ . Concluimos que  $x \equiv 2933 \pmod{11 \cdot 20 \cdot 21}$ .

- b. Aplicando el TCR a cada una de las congruencias vemos que

$$\begin{cases} x \equiv 7 \pmod{22} \\ x \equiv 21 \pmod{28} \\ x \equiv 23 \pmod{30} \end{cases} \Leftrightarrow \begin{cases} x \equiv 7 \pmod{11} \\ x \equiv 7 \pmod{2} \\ x \equiv 21 \pmod{4} \\ x \equiv 21 \pmod{7} \\ x \equiv 23 \pmod{2} \\ x \equiv 23 \pmod{3} \\ x \equiv 23 \pmod{5} \end{cases} \Leftrightarrow \begin{cases} x \equiv 7 \pmod{11} \\ x \equiv 1 \pmod{2} \\ x \equiv 1 \pmod{4} \\ x \equiv 0 \pmod{7} \\ x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \end{cases}.$$

Como  $x \equiv 1 \pmod{4}$  implica  $x \equiv 1 \pmod{2}$  vemos que el sistema es equivalente a

$$\begin{cases} x \equiv 7 \pmod{11} \\ x \equiv 1 \pmod{4} \\ x \equiv 0 \pmod{7} \\ x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \end{cases}.$$

Aplicando TRC a las congruencias 2 y 5 vemos que

$$\begin{cases} x \equiv 1 & (\text{mód } 4) \\ x \equiv 3 & (\text{mód } 5) \end{cases} \Leftrightarrow x \equiv 13 \pmod{20},$$

y lo mismo para las ecuaciones 3 y 4 para obtener

$$\begin{cases} x \equiv 0 & (\text{mód } 7) \\ x \equiv 2 & (\text{mód } 3) \end{cases} \Leftrightarrow x \equiv 14 \pmod{21}.$$

Por lo que el sistema queda equivalente al de la parte anterior y tiene la misma solución.