

EXAMEN - 16 DE DICIEMBRE DE 2015.

Ejercicio 1.

- a. Sea la función φ de Euler y dos enteros $m, n > 1$ tales que $\text{mcd}(m, n) = 1$. Probar que

$$\varphi(mn) = \varphi(m)\varphi(n).$$

- b. Mostrar con un ejemplo que lo anterior es falso si $\text{mcd}(m, n) \neq 1$.

- c. Calcular $\varphi(297)$.

- d. Reducir 629^{362} (mód 297).

Solución:

- a. Ver notas teóricas.

- b. Tomando $n = m = 2$ vemos que $\text{mcd}(m, n) = 2 \neq 1$ y $\varphi(4) = 2 \neq \varphi(2)\varphi(2) = 1$.

- c. Vemos que $297 = 3^3 \cdot 11$ por lo que $\varphi(297) = \varphi(3^3)\varphi(11) = 3^2(3-1)(11-1) = 180$.

- d. Vemos que $629 = 35 + 297 \cdot 2$ por lo que $629^{362} \equiv 35^{362} \pmod{297}$. Como 35 es coprimo con 297 podemos aplicar el teorema de Euler. Sabiendo que $362 = 2 + 180 \cdot 2$, llegamos a que

$$629^{362} \equiv 35^{362} \pmod{297} \equiv 35^2 \pmod{297} \equiv 1225 \pmod{297} \equiv 37 \pmod{297}.$$

Ejercicio 2.

- a. Sea G un grupo finito y $x, y \in G$ tales que $xy = yx$ y $\text{mcd}(\text{o}(x), \text{o}(y)) = 1$. Probar que

$$\text{o}(xy) = \text{o}(x) \text{o}(y).$$

- b. Sea $G = U(47)$ y $g = 2 \in G$. Probar que $\text{o}(g) = 23$.

- c. Utilizando lo anterior encontrar una raíz primitiva módulo 47.

- d. ¿El grupo $U(15)$ es cíclico? Justique su respuesta.

Solución:

- a. Ver notas teóricas.

- b. Como 47 es primo, $|G| = \varphi(47) = 46 = 2 \cdot 23$. Por el Teorema de Lagrange el orden de 2 puede ser 1, 2, 23, 46. Veamos que es efectivamente 23.

El orden de 2 no es 2 ya que $2^2 = 4 \not\equiv 1 \pmod{47}$. Alcanza con ver que $2^{23} \equiv 1 \pmod{47}$. Sabemos que $2^{10} = 1024 \equiv 37 \pmod{47}$. Por lo tanto $2^{23} = (2^{10})^2 2^3 \equiv 37^2 8 \pmod{47} \equiv 6 \cdot 8 \pmod{47} \equiv 1 \pmod{47}$.

- c. Viendo que $\text{o}(-1) = 2$ y $\text{o}(2) = 23$ son coprimos y estamos en un grupo abeliano, podemos concluir utilizando la parte a. que $\text{o}(-2) = \text{o}(2) \text{o}(-1) = 23 \cdot 2 = 46 = |G|$. Por lo tanto -2 es raíz primitiva módulo 47.

- d. Por el Teorema de la raíz primitiva sabemos que $U(p \cdot q)$ nunca es cíclico cuando p, q son dos primos impares distintos. Alternativamente se puede hallar los ordenes de los elementos de $U(15)$ y ver que ninguno tiene el orden de $U(15)$ que es $\varphi(15) = 8$.

A continuación vemos todos los ordenes: $\text{o}(1) = 1$, $\text{o}(2) = 4$, $\text{o}(4) = 2$, $\text{o}(7) = 4$, $\text{o}(8) = 4$, $\text{o}(11) = 2$, $\text{o}(13) = 4$, $\text{o}(14) = 2$.

Ejercicio 3.

- a. Sean $n = 253$ y $e = 9$. Para los datos anteriores hallar la función de descifrado $D : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ definida por el protocolo RSA.
- b. Reducir 22^{666} (mód 253).

Solución:

- a. El número $n = 253 = 11 \cdot 23$ por lo que $\varphi(n) = 10 \cdot 22 = 220$. La función de descifrado es $D(y) = y^d$ (mód n) donde $d \equiv e^{-1}$ (mód $\varphi(n)$), o sea $d \equiv 9^{-1}$ (mód 220). Utilizando el Algoritmo de Euclides Extendido obtenemos que $d \equiv 49$ (mód 220). Concluimos que $D(y) = y^{49}$ (mód 253).
- b. Como $22 = 2 \cdot 11$ no es coprimo con 253 no podemos aplicar el Teorema de Euler. Pero si podemos aplicar el Teorema Chino del Resto para hallar dicha potencia. Sabemos que

$$\begin{aligned} x \equiv 22^{666} \pmod{253} &\Leftrightarrow \begin{cases} x \equiv 22^{666} \pmod{11} \\ x \equiv 22^{666} \pmod{23} \end{cases} \Leftrightarrow \begin{cases} x \equiv 0 \pmod{11} \\ x \equiv (-1)^{666} \pmod{23} \end{cases} \Leftrightarrow \\ &\Leftrightarrow \begin{cases} x \equiv 0 \pmod{11} \\ x \equiv 1 \pmod{23} \end{cases} . \end{aligned}$$

Resolviendo obtenemos que $x \equiv 231$ (mód 253).

Ejercicio 4.

- a. i) Sean $n, m \in \mathbb{Z}$ tal que $n \mid m$ y $a, b \in \mathbb{Z}$. Probar que

$$a \equiv b \pmod{m} \implies a \equiv b \pmod{n}.$$

- ii) ¿Vale el recíproco de lo anterior? Justificar.

- b. Para el siguiente sistema investigar si tiene solución, y en caso de que tenga solución, hallar todas sus soluciones:

$$\begin{cases} x \equiv 17 \pmod{88} \\ x \equiv 83 \pmod{286} \end{cases} .$$

Solución:

- a. i) Ver notas teóricas.
- ii) Un contraejemplo de lo anterior es $n = 2$, $m = 4$ y $a = 1$, $b = 3$. Claramente $1 \equiv 3 \pmod{2}$ pero $1 \not\equiv 3 \pmod{4}$.
- b. Como los módulos del sistema no son coprimos no podemos aplicar directamente el Teorema Chino del Resto. Pero podemos aplicarlo a cada una de las congruencias y obtener

$$\begin{aligned} x \equiv 17 \pmod{88} &\Leftrightarrow \begin{cases} x \equiv 17 \pmod{8} \\ x \equiv 17 \pmod{11} \end{cases} \Leftrightarrow \begin{cases} x \equiv 1 \pmod{8} \\ x \equiv 6 \pmod{11} \end{cases} , \\ x \equiv 83 \pmod{286} &\Leftrightarrow \begin{cases} x \equiv 83 \pmod{2} \\ x \equiv 83 \pmod{11} \\ x \equiv 83 \pmod{13} \end{cases} \Leftrightarrow \begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 6 \pmod{11} \\ x \equiv 5 \pmod{13} \end{cases} . \end{aligned}$$

Uniendo toda esa información vemos que nuestro sistema con módulos no coprimos es equivalente a

$$\begin{cases} x \equiv 17 \pmod{88} \\ x \equiv 83 \pmod{286} \end{cases} \Leftrightarrow \begin{cases} x \equiv 1 \pmod{8} \\ x \equiv 6 \pmod{11} \\ x \equiv 5 \pmod{13} \end{cases} ,$$

ya que las congruencias son todas compatibles. Una solución al sistema anterior utilizando el algoritmo para resolver sistemas es $x \equiv 369$ (mód $8 \cdot 11 \cdot 13$).