

Primera parte: Múltiple Opción

MO	
1	2

Ejercicio 1. Sean $n = 319$ y $e = 19$. Para los datos anteriores sea función de descifrado $D : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ definida por el protocolo RSA. Indicar cuál de las opciones es correcta:

- A. $D(y) = y^{42} \pmod n$.
- B. $D(y) = y^{59} \pmod n$.
- C. $D(y) = y^{84} \pmod n$.
- D. $D(y) = y^{67} \pmod n$.

La función de descifrado es $D(y) = y^d \pmod n$ donde d es tal que $d \equiv e^{-1} \pmod{\varphi(n)}$. La factorización de n es $319 = 11 \cdot 29$, por lo que $\varphi(11 \cdot 29) = 10 \cdot 28 = 280$. Utilizando el algoritmo extendido de Euclides obtenemos $d \equiv 59 \pmod{280}$.

Ejercicio 2. Sea $0 \leq m < 325$ tal que $m \equiv 435^{241} \pmod{325}$. Indicar cuál de las opciones es correcta:

- A. $m = 65$.
- B. $m = 110$.
- C. $m = 300$.
- D. $m = 175$.

Como $435 = 3 \cdot 5 \cdot 29$ no es coprimo con $325 = 5^2 \cdot 13$ no podemos aplicar el Teorema de Euler. Aplicando el Teorema Chino del Resto obtenemos

$$x \equiv 435^{241} \pmod{325} \Leftrightarrow \begin{cases} x \equiv 435^{241} \pmod{5^2} \\ x \equiv 435^{241} \pmod{13} \end{cases} \Leftrightarrow \begin{cases} x \equiv 5^{241}(3 \cdot 29)^{241} \pmod{5^2} \\ x \equiv 6^{241} \pmod{13} \end{cases} .$$

Ahora como $5^2 \mid 5^{241}$ entonces $435^{241} \equiv 0 \pmod{5^2}$. Por otro lado $\varphi(13) = 12$ y como 6 y 13 son coprimos, por el teorema de Euler tenemos que $6^{12} \equiv 1 \pmod{13}$, por lo que $6^{241} = 6^{12 \cdot 20 + 1} \equiv 6 \pmod{13}$. Concluimos que

$$x \equiv 435^{241} \pmod{325} \Leftrightarrow \begin{cases} x \equiv 0 \pmod{5^2} \\ x \equiv 6 \pmod{13} \end{cases} ,$$

que tiene solución $x \equiv 175 \pmod{325}$. Por lo que $m = 175$.

Segunda parte: Desarrollo

Ejercicio 3. Dado los siguientes sistemas, investigar si tienen solución, y en caso que tenga encontrar todas sus respectivas soluciones.

a. $\begin{cases} x \equiv 2 \pmod{11} \\ x \equiv 5 \pmod{8} \\ x \equiv 14 \pmod{15} \end{cases} .$

Como 11, 8 y 15 son coprimos dos a dos, por el Teorema Chino de Resto sabemos que existe solución y que es única módulo $11 \cdot 8 \cdot 15 = 1320$; es decir que existe una solución x_0 y todas las soluciones son $x \equiv x_0 \pmod{1320}$.

Si realizamos el cambio de variable $x' = x - 14$, el sistema en esta variable nos queda:

$$\begin{cases} x' \equiv -12 \pmod{11} \equiv -1 \pmod{11} \\ x' \equiv -9 \pmod{8} \equiv -1 \pmod{8} \\ x' \equiv 10 \pmod{15} \end{cases}$$

que equivale a
$$\begin{cases} x' \equiv -1 \pmod{88} \\ x' \equiv 10 \pmod{15} \end{cases} .$$

Es decir $x' = -1 + 88k$ con $k \in \mathbb{Z}$ y $-1 + 88k \equiv 0 \pmod{15}$. Entonces $13k \equiv 1 \pmod{15} \Rightarrow -2k \equiv 1 \pmod{15} \Rightarrow k \equiv 7 \pmod{15}$. Es decir $k = 7 + 15z : z \in \mathbb{Z}$. Entonces $x' = -1 + 88(7 + 15z) = 615 + 1320z$ y $x = x' + 14 = 629 + 1320z, z \in \mathbb{Z}$.

b.
$$\begin{cases} x \equiv 9 \pmod{20} \\ x \equiv 5 \pmod{24} \\ x \equiv 35 \pmod{66} \end{cases} .$$

Por el Teorema Chino del resto, tenemos que $x \equiv 9 \pmod{20}$ si y sólo si
$$\begin{cases} x \equiv 9 \pmod{4} \equiv 1 \pmod{4} \\ x \equiv 9 \pmod{5} \equiv 4 \pmod{5} \end{cases} .$$

De forma análoga, tenemos que $x \equiv 5 \pmod{24}$ si y sólo si
$$\begin{cases} x \equiv 5 \pmod{8} \\ x \equiv 5 \pmod{3} \equiv 2 \pmod{3} \end{cases} ,$$

y que $x \equiv 35 \pmod{66}$ es equivalente a

$$\begin{cases} x \equiv 35 \pmod{2} \equiv 1 \pmod{2} \\ x \equiv 35 \pmod{3} \equiv 2 \pmod{3} \\ x \equiv 35 \pmod{11} \equiv 2 \pmod{11} \end{cases} .$$

Entonces el sistema original es equivalente a

$$\begin{cases} x \equiv 1 \pmod{4} \\ x \equiv 4 \pmod{5} \\ x \equiv 5 \pmod{8} \\ x \equiv 2 \pmod{3} \\ x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{11} \end{cases} .$$

Ahora si $x \equiv 5 \pmod{8}$ entonces $x \equiv 5 \pmod{4} \equiv 1 \pmod{4}$ y $x \equiv 1 \pmod{2}$; por lo que la tercer ecuación

implica la primera y la penúltima; y el sistema resulta equivalente a
$$\begin{cases} x \equiv 4 \pmod{5} \\ x \equiv 5 \pmod{8} \\ x \equiv 2 \pmod{3} \\ x \equiv 2 \pmod{11} \end{cases} .$$

Y como (por el Teo. Chino del Resto)
$$\begin{cases} x \equiv 4 \pmod{5} \\ x \equiv 2 \pmod{3} \end{cases}$$
 equivale a $x \equiv 14 \pmod{15}$; obtenemos que el sistema original es equivalente al sistema
$$\begin{cases} x \equiv 14 \pmod{15} \\ x \equiv 5 \pmod{8} \\ x \equiv 2 \pmod{11} \end{cases} ,$$
 que es el sistema resuelto en la parte anterior.

Ejercicio 4.

a. Definir la función $\varphi : \mathbb{N}^+ \rightarrow \mathbb{N}$ de Euler.

Ver teórico, definición 2.6.1.

b. Probar que si $\text{mcd}(n, m) = 1$ entonces

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

Ver teórico Teorema 2.6.3.

c. Calcular:

i) $\varphi(125)$.

$$\varphi(125) = \varphi(5^3) = 5^3 - 5^2 = 100.$$

ii) $\varphi(108)$.

$$\varphi(108) = \varphi(2^2 \cdot 3^3) = \varphi(2^2)\varphi(3^3) = (2^2 - 2)(3^3 - 3^2) = 2 \cdot 18 = 36$$

d. Sabiendo que 2 es raíz primitiva módulo 25 y 125, hallar todos los homomorfismos

$$f : U(125) \rightarrow U(25).$$

Como $U(125) = \langle \bar{2} \rangle$, por la proposición 3.9.9 de teórico, tenemos que todo morfismo $f : U(125) \rightarrow K$ es de la forma $f(\bar{2}^x) = f(\bar{2})^x$ con la condición de que $o(f(\bar{2})) \mid o(\bar{2})$. Ahora, como 2 es raíz primitiva módulo 125, el orden de $\bar{2}$ en $U(125)$ es $\varphi(125) = 100$. Entonces cada morfismo está determinado por la elección de $y = f(\bar{2}) \in U(25)$ tal que $o(y) \mid 100$. Ahora por el Corolario 3.8.2, tenemos que $o(y) \mid |U(25)| = \varphi(25) = 20$ para todo $y \in U(25)$. Por lo que $o(y) \mid 100$ para todo $y \in U(25)$.

Entonces, existen tantos morfismos como elementos de $U(25)$. Es decir, hay 20 homomorfismos.

Ejercicio 5.

- a. Sea G un grupo finito, y $g \in G$ tal que $o(g) = m$. Probar que

$$o(g^k) = \frac{m}{\text{mcd}(k, m)}.$$

Ver teórico (Proposición 3.7.8)

- b. Probar que si existe una raíz primitiva módulo n entonces hay exactamente $\varphi(\varphi(n))$ raíces primitivas módulo n . Ver teórico (proposición 4.1.3)

- c. Sea p un primo y g una raíz primitiva módulo p .

- i) Probar que si n es el orden de g en $U(p^2)$ entonces $p - 1 \mid n$.

Si $n = o(g)$ en $U(p^2)$, en particular $g^n \equiv 1 \pmod{p^2}$ es decir que $p^2 \mid g^n - 1$ y entonces $p \mid g^n - 1$. Por lo tanto $g^n \equiv 1 \pmod{p}$ y entonces si m es el orden de g en $U(p)$ tenemos que $m \mid n$.

- ii) Probar que g o $g + p$ es raíz primitiva módulo p^2 .

Por ser g raíz primitiva módulo p , sabemos que en $U(p)$ el orden de g es $p - 1$. Por la parte anterior, tenemos que si n es el orden de g en $U(p^2)$ entonces $p - 1 \mid n$. Por otro lado, $n \mid |U(p^2)| = \varphi(p^2) = p(p - 1)$.

Por lo tanto, $p - 1 \mid n$ y $n \mid p(p - 1)$; al ser p primo tenemos que $n = p - 1$ o $n = p(p - 1)$. Si $n = p(p - 1)$ entonces g es raíz primitiva módulo p^2 .

Veamos ahora qué pasa si $n = p - 1$. Llamemos m al orden de $g + p$ en $U(p^2)$. Tenemos entonces que $m \mid p(p - 1)$ y como $(g + p)^m \equiv 1 \pmod{p^2} \Rightarrow (g + p)^m \equiv 1 \pmod{p} \Rightarrow g^m \equiv 1 \pmod{p}$ tenemos que $p - 1 \mid m$. Es decir que $m = p - 1$ o $m = p(p - 1)$. Ahora

$$(g + p)^{p-1} = g^{p-1} + (p-1)g^{p-2}p + \sum_{i=2}^{p-1} \binom{p-1}{i} g^{p-1-i} p^i \equiv g^{p-1} + (p-1)g^{p-2}p \pmod{p^2}.$$

Como $n = p - 1$, tenemos que $g^{p-1} \equiv 1 \pmod{p^2}$ y entonces $(g + p)^{p-1} \equiv 1 + (p - 1)g^{p-2}p \pmod{p^2} \equiv 1 - g^{p-2}p \pmod{p^2}$. Como g es coprimo con p , $p \nmid g$ y entonces $p^2 \nmid g^{p-2}p$; por lo que $g^{p-2}p \not\equiv 0 \pmod{p^2}$ y entonces $(g + p)^{p-1} \not\equiv 1 \pmod{p^2}$. Concluimos entonces que $m \neq p - 1$, y entonces $m = p(p - 1)$ de lo que resulta que $g + p$ es raíz primitiva módulo p^2 .

- d. Hallar una raíz primitiva módulo 11^2 .

Hallemos primero una raíz primitiva módulo 11. Como $\varphi(11) = 10 = 2 \times 5$, tenemos que g es raíz primitiva módulo 11, si y sólo si $\text{mcd}(g, 11) = 1$ y $g^5 \not\equiv 1 \pmod{11}$ y $g^2 \not\equiv 1 \pmod{11}$.

Probando con $g = 2$, tenemos que $2^2 = 4 \not\equiv 1 \pmod{11}$ y que $2^5 = 32 \equiv 10 \pmod{11} \not\equiv 1 \pmod{11}$. Por lo tanto 2 es raíz primitiva módulo 11.

Por la parte anterior, tenemos que 2 o 13 es raíz primitiva módulo 11^2 y que los órdenes de estos elementos en $U(11^2)$ son 10 o $11 \cdot 10$. Como $2^{10} = 2^7 2^3 = 128 \cdot 8 \equiv 7 \cdot 8 \pmod{121} \equiv 56 \pmod{121} \not\equiv 1 \pmod{121}$, concluimos que el orden de 2 en $U(11^2)$ no es 10 y por lo tanto es $11 \cdot 10$. Y entonces 2 es raíz primitiva módulo 11^2 .