

SOLUCIÓN DEL EXAMEN - 17 DE FEBRERO DE 2016.

**Ejercicio 1.**

- a. Dados  $p, q, n, d$  y  $e$  en las hipótesis del criptosistema RSA y las funciones de cifrado  $E(x) = x^e \pmod{n}$  y descifrado  $D(y) = y^d \pmod{n}$ . Probar que la función de descifrado funciona como tal; es decir, probar que:

$$D(E(x)) = x \pmod{n} \quad \forall x \in \mathbb{Z}_n.$$

- b. Dados los primos  $p = 17$ ,  $q = 19$  y  $e = 11$ , calcular la función de descifrado  $D$ .  
c. Con los mismos datos que en (b) cifrar  $x = 170$ .

**Solución:**

- a. Ver notas teóricas (Proposición 5.3.1 de los apuntes de teórico).  
b.  $n = pq = 17(19) = 323$ ;  $\varphi(n) = 16(18) = 288$ . La función de descifrado es  $D(y) = y^d \pmod{n}$  siendo  $d$  tal que  $ed \equiv 1 \pmod{\varphi(n)}$ . Buscamos entonces  $d$  tal que  $11d \equiv 1 \pmod{288}$ . Realizando el algoritmo de Euclides extendido para 288 y 11 obtenemos que  $11(131) - 5(288) = 1$  y por lo tanto  $11(131) \equiv 1 \pmod{288}$  y entonces  $d = 131$ .

- c. Debemos calcular  $y = E(170) = 170^{11} \pmod{323}$ . Como 17 y 19 son coprimos, esto equivale a hallar  $y$  tal que

$$\begin{cases} y \equiv 170^{11} \pmod{17} \\ y \equiv 170^{11} \pmod{19}. \end{cases}$$

Es decir

$$\begin{cases} y \equiv 0 \pmod{17} \\ y \equiv (-1)^{11} \pmod{19} \equiv -1 \pmod{19}, \end{cases}$$

y por lo tanto  $y = 170$ ; es decir  $E(170) = 170$ .

**Ejercicio 2.** Sea  $G$  un grupo y  $g \in G$ .

- a. Probar que  $\langle g \rangle := \{g^n : n \in \mathbb{Z}\}$  es un subgrupo de  $G$ .  
b. Probar que  $|\langle g \rangle| = o(g)$   
c. Si  $G$  es finito, probar que  $g^{|G|} = e_G$ .

**Solución:** Ver notas teóricas (Proposición 3.7.4, 3.7.9 y parte (2) del Corolario 3.8.2).

**Ejercicio 3.**

- a. Hallar todas las soluciones módulo 61 de la ecuación  $3x \equiv 10 \pmod{61}$ .  
b. Sea la ecuación

$$4x \equiv 20 \pmod{100}. \tag{1}$$

- i) Hallar todas las soluciones módulo 100 de la ecuación (1).  
ii) Hallar todas sus soluciones módulo 50 y 25 de la ecuación (1).  
iii) ¿Cuántas soluciones módulo 1000 tiene la ecuación (1)?

**Solución:**

- a.  $3x \equiv 10 \pmod{61} \Leftrightarrow \exists y \in \mathbb{Z} : 3x - 61y = 10$ . Realizando el algoritmo de Euclides extendido obtenemos que  $3(41) - 61(2) = 1$  y por lo tanto,  $3(410) - 61(20) = 10$ . Por el teorema de ecuaciones diofánticas, como  $\text{mcd}(3, 61) = 1$  tenemos que todas las soluciones de  $3x - 61y = 10$  son  $(x, y) = (410 + 61k, 20 + 3k)$ ,  $k \in \mathbb{Z}$ . Por lo tanto todas las soluciones de la ecuación  $3x \equiv 10 \pmod{61}$  son  $x = 410 + 61k$ ,  $k \in \mathbb{Z}$ ; es decir, hay una única solución módulo 61,  $x \equiv 410 \pmod{61} \equiv 44 \pmod{61}$ .

Otra forma de resolverlo es, como  $\text{mcd}(3, 61) = 1$ , 3 es invertible módulo 61. Hallamos primero el inverso de 3 módulo 61: como  $3(41) - 61(2) = 1$  resulta que  $3(41) \equiv 1 \pmod{61}$  y por lo tanto  $3^{-1} \equiv 41 \pmod{61}$ . Entonces  $3x \equiv 10 \pmod{61} \Leftrightarrow x \equiv 10(41) \pmod{61} \equiv 410 \pmod{61} \equiv 44 \pmod{61}$ .

Otra forma, es notando que  $10 \equiv -51 \pmod{61} \equiv 3(-17) \pmod{61}$  y como  $\text{mcd}(3, 61) = 1$ , podemos cancelar el 3 de la ecuación módulo 61. Es decir,  $3x \equiv 10 \pmod{61} \Leftrightarrow 3x \equiv 3(-17) \pmod{61} \Leftrightarrow x \equiv (-17) \pmod{61} \equiv 44 \pmod{61}$ .

- b. Como  $\text{mcd}(4, 100) = 4$  y  $4 \mid 20$ , el teorema de ecuaciones con congruencias (Teorema 2.4.2 de los apuntes) nos dice que la ecuación tienen solución y además que hay exactamente  $\text{mcd}(4, 100) = 4$  soluciones distintas módulo 100. Como  $\text{mcd}(4, 100) = 4 \neq 1$  no se puede cancelar el 4 en la ecuación módulo 100; la cancelativa que podemos aplicar es la que dice que si  $c \mid n$  entonces  $ca \equiv cb \pmod{n} \Leftrightarrow a \equiv b \pmod{\frac{n}{c}}$  (ítem 2 de la Proposición 2.2.4 de los apuntes). Por lo tanto, cancelando el 4 obtenemos

$$4x \equiv 20 \pmod{100} \Leftrightarrow x \equiv 5 \pmod{25} \Leftrightarrow x = 5 + 25k, k \in \mathbb{Z}.$$

- i) Por lo dicho antes, hay 4 soluciones distintas módulo 100 y por la cuenta anterior tenemos que ellas son  $x_1 = 5$ ,  $x_2 = 5 + 25 = 30$ ,  $x_3 = 5 + 2(25) = 55$  y  $x_4 = 5 + 3(25) = 80$ .
- ii) Como vimos antes, la ecuación es equivalente a  $x \equiv 5 \pmod{25}$  y por lo tanto  $x = 5$  es la única solución módulo 25. Como las soluciones son  $x = 5 + 25k$ ,  $k \in \mathbb{Z}$  tenemos que o  $x = 5 + 50k$  o  $x = 30 + 50k$ ,  $k \in \mathbb{Z}$ ; por lo tanto hay dos soluciones módulo 50, ellas son  $x_1 = 5$  y  $x_2 = 30$ .
- iii) Como  $1000 = 25(40)$ , y las soluciones son de la forma  $x = 5 + 25k$ ,  $k \in \mathbb{Z}$ ; las (40) soluciones obtenidas con  $k = 0, 1, \dots, 39$  no son congruentes entre sí módulo 1000 (ya que la diferencia entre cualquier par de ellas es menor que 1000), y además, cualquier otra solución será congruente con una de éstas módulo 1000. Pues si  $x = 5 + 25k$  y  $k = 40q + r$  con  $r \in \{0, 1, \dots, 39\}$  entonces  $x = 5 + 25k = 5 + 25(40q + r) = 5 + 1000q + 25r \equiv 5 + 25r \pmod{1000}$ . Por lo tanto hay exactamente 40 soluciones distintas módulo 1000.

#### Ejercicio 4.

- a. Probar que 2 es raíz primitiva módulo 59.
- b. Hallar el orden de 57 módulo 59.
- c. Encontrar todos los homomorfismos  $f : U(59) \rightarrow S_3$ .
- d. Hallar una raíz primitiva módulo 118.

#### Solución:

- a. Como  $\text{mcd}(2, 59) = 1$  y  $\varphi(59) = 58 = 2 \times 29$ , por la parte 3 (o 4) de la Proposición 4.1.4 de los apuntes, tenemos que 2 es raíz primitiva módulo 59 si y sólo si  $2^2 \not\equiv 1 \pmod{59}$  y  $2^{29} \not\equiv 1 \pmod{59}$ .  
Tenemos que  $2^2 = 4 \not\equiv 1 \pmod{59}$  y que  $2^4 = 16$ ,  $2^8 = 16^2 = 256 \equiv 20 \pmod{59}$ ,  $2^{16} \equiv 20^2 \pmod{59} \equiv 400 \pmod{59} \equiv 46 \pmod{59}$ ; por lo tanto  $2^{29} = 2^{16} 2^8 2^4 2 \equiv 46 \times 20 \times 16 \times 2 \pmod{59} \equiv 58 \pmod{59} \equiv -1 \pmod{59} \not\equiv 1 \pmod{59}$ . Por lo tanto 2 es raíz primitiva módulo 59.
- b. Como  $|U(59)| = 58 = 2 \times 29$  y para todo  $g \in U(59)$ ,  $o(g)$  divide a  $|U(59)|$ , tenemos que las posibilidades para  $o(57)$  son 1, 2, 29 y 58. Como  $57 \not\equiv 1 \pmod{59}$  y  $57^2 \equiv (-2)^2 \pmod{59} \equiv 4 \pmod{59} \not\equiv 1 \pmod{59}$ , tenemos que  $o(57) \neq 1, 2$ .  
Por otro lado,  $57^{29} \equiv (-2)^{29} \pmod{59} \equiv (-1)^{29} 2^{29} \pmod{59} \equiv (-1)(-1) \pmod{59} \equiv 1 \pmod{59}$ ; por lo tanto,  $o(57) = 29$ .
- c. Por la parte a) tenemos que  $U(59)$  es cíclico y generado por 2. Por lo tanto, todo elemento de  $U(59)$  es de la forma  $2^k$ , y entonces para dar un homomorfismo  $f : U(59) \rightarrow S_3$ , basta con dar la imagen de 2; ya que luego  $g(2^k) = f(2)^k$ . Por la proposición 3.9.9, para que el homomorfismo esté bien definido, basta con dar  $f(2) \in S_3$  tal que  $o(f(2)) \mid o(2)$ ; es decir  $f(2)$  tal que  $f(2) \mid 58$ . Como los elementos de  $S_3$  tienen orden 1, 2 o 3, las posibilidades para  $o(f(2))$  son 1 y 2. El único elemento de  $S_3$  con orden 1, es el neutro  $e = Id$ ; y los elementos de  $S_3$  con orden 2 son  $\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ ,  $\tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ ,  $\tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ .  
Entonces hay cuatro homomorfismos  $f : U(59) \rightarrow S_3$ ; ellos son  $f(2^k) = Id$ ,  $f(2^k) = \tau_1^k$ ,  $f(2^k) = \tau_2^k$  y  $f(2^k) = \tau_3^k$ .
- d. Como  $118 = 2 \times 59$ , 59 es primo, 2 es raíz primitiva módulo 59 y 2 es par; por el Lema 4.1.13 tenemos que  $2 + 59$  es raíz primitiva módulo  $2 \times 59$ ; es decir que 61 es raíz primitiva módulo 118.