Soluciones

2. Semana 2

2.1. Inversos modulares. Teorema chino del resto. Cifrado afín II

1. *a*) $3^{-1} \equiv 9 \mod 26$. Comprobación: $3 \cdot 9 = 27 \equiv 1 \mod 26$.

   b) $\nexists\, 22^{-1} \mod 28$.

   c) $15^{-1} \equiv 15 \mod 28$. Comprobación: $15 \cdot 15 = 225 \equiv 1 \mod 28$.

2. De la primera ecuación: $b \equiv 23 - 4a \mod 26$.

   Restando la primera ecuación de la segunda: $15a \equiv -3 \equiv 23 \mod 26$.

   $$15a \equiv 23 \mod 26 \Rightarrow a \equiv 15^{-1} \cdot 23 \equiv 7 \cdot 23 \equiv 5 \mod 26,$$

   $$a \equiv 5 \mod 26, \quad b \equiv 3 \mod 26.$$

3. *a*) $4x \equiv 4y \mod 28 \Leftrightarrow 28 \mid (4x - 4y) \Leftrightarrow$
   existe un entero k tal que $4x - 4y = 28k \Leftrightarrow$
   existe un entero k tal que $x - y = 7k \Leftrightarrow$
   $7 \mid (x - y) \Leftrightarrow x \equiv y \mod 7$.

   b) (i) $4a' \equiv 4 \mod 28 \Leftrightarrow a' \equiv 1 \mod 7$.
   Por tanto las soluciones son

   $$a' \equiv 1 \mod 28 \quad \text{ó} \quad a' \equiv 8 \mod 28$$

   $$\text{ó} \quad a' \equiv 15 \mod 28 \quad \text{ó} \quad a' \equiv 22 \mod 28.$$

   (ii) $12a' \equiv 8 \mod 28 \Leftrightarrow 3a' \equiv 2 \mod 7 \Leftrightarrow a' \equiv 3^{-1} \cdot 2 \mod 7$.

   $$a' \equiv 5 \cdot 2 \equiv 10 \equiv 3 \mod 7.$$

   Por tanto las soluciones son

   $$a' \equiv 3 \mod 28 \quad \text{ó} \quad a' \equiv 10 \mod 28$$

   $$\text{ó} \quad a' \equiv 17 \mod 28 \quad \text{ó} \quad a' \equiv 24 \mod 28.$$

4. *a*) $(\mathbb{Z}_{12}, +)$ es un grupo conmutativo: $(+)$ es asociativa, conmutativa, tiene elemento neutro (0) y todo elemento $a \in \mathbb{Z}_{12}$ tiene simétrico para $(+)$ (opuesto): el opuesto de a es $12 - a \in \mathbb{Z}_{12}$.
   $(\mathbb{Z}_{12} \setminus \{0\}, \cdot)$ no es un grupo conmutativo porque no todo elemento tiene simétrico para $(\cdot)$ (inverso). Por ejemplo, no existe $2^{-1} \mod 12$ porque $\text{mcd}(2, 12) \neq 1$. Por tanto, $(\mathbb{Z}_{12}, +, \cdot)$ no es cuerpo.

b) $2 \cdot 6 \equiv 3 \cdot 4 \equiv 3 \cdot 8 \equiv 4 \cdot 6 \equiv 4 \cdot 9 \equiv 6 \cdot 6 \equiv 6 \cdot 8 \equiv 6 \cdot 10$
$\equiv 8 \cdot 9 \equiv 0 \mod 12$.

c) $\phi(12) = 4$.

d) $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$. $(\mathbb{Z}_{12}^*, \cdot)$ es grupo: $(\cdot)$ es asociativa, tiene elemento neutro (1) y todo elemento $a \in \mathbb{Z}_{12}^*$ tiene simétrico para $(\cdot)$ (inverso).

5. *a*) $4^{10} \equiv 1 \mod 11$, $5^{10} \equiv 1 \mod 11$.
$5^{20} \equiv 1 \mod 11$, $5^{21} \equiv 5 \mod 11$.
(Hay que tener en cuenta que $5^{20} = (5^{10})^2$).

b) $19^{186} \equiv 32 \mod 47$.
(Hay que tener en cuenta que $19^{186} = 19^{46 \cdot 4 + 2} = (19^{46})^4 \cdot 19^2$).

6. *a*) $\phi(85) = 16 \cdot 4 = 64$.

b) $11^{64} \equiv 1 \mod 85$, $11^{129} \equiv 11 \mod 85$.
(Hay que tener en cuenta que $11^{129} = 11^{64 \cdot 2 + 1} = (11^{64})^2 \cdot 11$).

7. *a*) Sea $a \equiv a_p \mod p$ y $x \equiv x_p \mod (p-1)$. Hay que probar

$$a^x \equiv a_p^{x_p} \mod p.$$

$$a^x \equiv \overbrace{a \cdot a \cdot \cdots \cdot a}^{x \text{ veces}} \equiv \overbrace{(a \mod p) \cdot \cdots \cdot (a \mod p)}^{x \text{ veces}} \equiv \overbrace{a_p \cdot \cdots \cdot a_p}^{x \text{ veces}} \equiv a_p^x \mod p.$$

$$x \equiv x_p \mod (p-1) \Rightarrow x = k(p-1) + x_p, \text{ con } k \text{ entero.}$$

$$a^x \equiv a_p^x \equiv a_p^{k(p-1)+x_p} \equiv a_p^{k(p-1)} \cdot a_p^{x_p} \equiv (a_p^{(p-1)})^k \cdot a_p^{x_p} \mod p.$$

- Si $\mathrm{mcd}(a_p, p) = 1$, entonces por el pequeño Teorema de Fermat, $a_p^{(p-1)} \equiv 1 \mod p$. Por tanto,

$$a^x \equiv a_p^x \equiv (a_p^{(p-1)})^k \cdot a_p^{x_p} \equiv 1^k \cdot a_p^{x_p} \equiv a_p^{x_p} \mod p.$$

- Si $\mathrm{mcd}(a_p, p) \neq 1$ entonces, como p es primo, $\mathrm{mcd}(a_p, p) = p$. Luego $p \mid a_p$ y, por tanto, $a \equiv a_p \equiv 0 \mod p$. Por tanto, en este caso,

$$a^x \equiv a_p^{x_p} \equiv 0 \mod p.$$

b) $1002^{34} \equiv 4 \mod 5$.

8. $x = qq_1a + pp_1b \equiv (qq_1 \mod p)a + (pp_1 \mod p)b \equiv 1 \cdot a + 0 \cdot b \equiv a \mod p$.
Análogamente,
$x = qq_1a + pp_1b \equiv (qq_1 \mod q)a + (pp_1 \mod q)b \equiv 0 \cdot a + 1 \cdot b \equiv b \mod q$.

9. $x \equiv 35 \mod 60$.

   Comprobación:

$$\begin{array}{ccccc} 35 \equiv 3 \mod 4, & & 35 \equiv 2 \mod 3, & & 35 \equiv 0 \mod 5, \\ 95 \equiv 3 \mod 4, & & 95 \equiv 2 \mod 3, & & 95 \equiv 0 \mod 5, \\ -25 \equiv 3 \mod 4, & & -25 \equiv 2 \mod 3, & & -25 \equiv 0 \mod 5, \end{array}$$

$$\vdots$$

10. $x \equiv 40 \mod 42$.

    Comprobación: $40 \equiv 5 \mod 7$, $40 \equiv 4 \mod 6$.

    También $82 \equiv 5 \mod 7$, $82 \equiv 4 \mod 6$, etc.

11. *a*) $(a', b') = (15, 19)$.

    b) "CRIPTOANALISIS".

12. $b' = 10$, "ELDIAD".

13. $(a', b') = (397, 269)$, "CRIPTO".

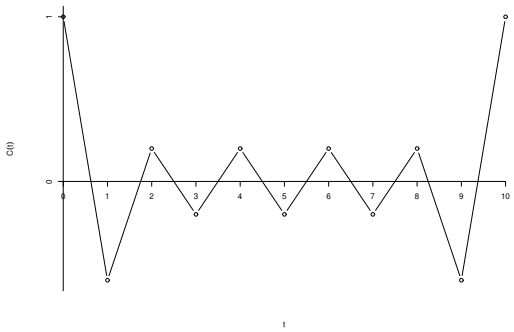
14. $(a', b') = (23, 33)$, "ES UN PROBLEMA".

2.2. Características del cifrado en flujo. Generación de secuencias pseudoaleatorias

1. Clave = 1011101010. $M_2 = 01100000$.

2.

$$\begin{array}{l} \mathrm{C}(0) = \mathrm{C}(10) = 1 \\ \mathrm{C}(1) = \mathrm{C}(9) = -3/5 \\ \mathrm{C}(2) = \mathrm{C}(8) = 1/5 \\ \mathrm{C}(3) = \mathrm{C}(7) = -1/5 \\ \mathrm{C}(4) = \mathrm{C}(6) = 1/5 \\ \mathrm{C}(5) = -1/5 \end{array}$$



3.

$$\sum_{i=0}^{t-1}(2s_i-1)(2s_{i+T-t}-1) = \sum_{j=T-t}^{T-1}(2s_{j+t-T}-1)(2s_j-1) = \sum_{j=T-t}^{T-1}(2s_{j+t}-1)(2s_j-1),$$

$$\sum_{i=t}^{T-1}(2s_i-1)(2s_{i+T-t}-1) = \sum_{j=0}^{T-t-1}(2s_{j+t}-1)(2s_{j+T}-1) = \sum_{j=0}^{T-t-1}(2s_{j+t}-1)(2s_j-1).$$

Por tanto,

$$\begin{aligned}\mathrm{C}(T-t) &= \frac{1}{T}\left(\sum_{i=0}^{t-1}(2s_i-1)(2s_{i+T-t}-1)+\sum_{i=t}^{T-1}(2s_i-1)(2s_{i+T-t}-1)\right)\\ &= \frac{1}{T}\left(\sum_{j=T-t}^{T-1}(2s_{j+t}-1)(2s_j-1)+\sum_{j=0}^{T-t-1}(2s_{j+t}-1)(2s_j-1)\right)\\ &= \frac{1}{T}\sum_{j=0}^{T-1}(2s_{j+t}-1)(2s_j-1) = \mathrm{C}(t).\end{aligned}$$

2.3. Generadores congruenciales

1. *a*) $a = 2 \not\equiv 1 \mod 13$. Por tanto, las secuencias que origina no poseen período máximo.

   b) $4|12$ y $a = 7 \equiv 3 \not\equiv 1 \mod 4$. Por tanto, las secuencias que origina no poseen período máximo.

2. *a*) $1, 6, 2, 8, 6, 2, 8, 6, \ldots$. Período=3, preperíodo= 1. No presenta período máximo.

   $\mathrm{mcd}(b, m) = 2 \neq 1$. Además, los divisores primos de 14 son 2, 7 y $2 \equiv 0 \not\equiv 1 \mod 2$, $2 \equiv 2 \not\equiv 1 \mod 7$.

   b) $2, 10, 16, 16, \ldots$. Período=1, preperíodo= 2. No presenta período máximo.

   $\mathrm{mcd}(b, m) = 2 \neq 1$. Además, los divisores primos de 18 son 2, 3 y $3 \equiv 0 \not\equiv 1 \mod 3$.

   c) $1, 4, 7, 10, 0, 3, 6, 9, 12, 2, 5, 8, 11, 1, \ldots$ Período: 13, preperíodo: 0.

3. $a = 1$ o $a = 31$ o $a = 61$.

4. $x_3 = 16, \quad x_4 = 9$.