HOJA 1 - CÓDIGOS

$\boxed{1.}$ Propiedad 1

Escribimos el DNI como:

$N = a_7 10^7 + a_6 10^6 + a_5 10^5 + a_4 10^4 + a_3 10^3 + a_2 10^2 + a_1 10 + a_0$

$a_i \in \mathbb{Z}$ y $0 \leq a_i \leq 9$

Supongamos que se ha cometido un error en la posición i de manera que en lugar de escribir la cifra a_i se ha escrito la cifra $(a_i + e)$, $e \in \mathbb{Z}$ con $-a_i \leq e \leq 9 - a_i$.

Llamemos N_e al nº del DNI con un error en el lugar i:

$N_e = a_7 10^7 + a_6 10^6 + a_5 10^5 + a_4 10^4 + a_3 10^3 + a_2 10^2 + a_1 10 + a_0 + e 10^i = N + e 10^i$

No detectaríamos el error si $N \equiv N_e \pmod{24} \Leftrightarrow N \equiv N + e 10^i \pmod{24}$

$\Leftrightarrow e 10^i \equiv 0 \pmod{24}$

El problema es que 10 y 24 no son coprimos y entonces puede que no se detectasen ciertos errores.

Por ejemplo, si $a_i = 2$ en la posición $i=2$ no detectaría un error $e = 6$ porque $6 \cdot 10^2 = 600 \equiv 0 \pmod{24}$

Propiedad 2

Supongamos que se han permutado las cifras de las posiciones i e $i+1$, $0 \leq i \leq 6$. Para no detectar el error la letra asignada tiene que ser la misma:

$N \equiv N_e \pmod{24} \Leftrightarrow N - N_e \equiv 0 \pmod{24}$

$N - N_e = (a_{i+1} - a_i) 10^{i+1} + (a_i - a_{i+1}) 10^i = (a_{i+1} - a_i) 10^i \cdot 9 \equiv 0 \pmod{24}$

De nuevo, $10^i \cdot 9$ no es coprimo con 24 y pueden no detectarse errores. Por ejemplo, para una permutación en la 2ª y 3ª cifra (e.d. $i=2$) donde $a_{i+1} - a_i = 2$ ó múltiplo de 2 tenemos

$2k \cdot 10^2 \cdot 9 = 1800k \equiv 0 \pmod{24}$ para $k \in \mathbb{N}$

Propiedad 4

Supongamos que la cifra que está en la posición i es ilegible, pero conocemos las 7 cifras restantes y la letra (el resto mod. 24 del DNI).

Tenemos $N = a_7 10^7 + a_6 10^6 + a_5 10^5 + a_4 10^4 + a_3 10^3 + a_2 10^2 + a_1 10 + a_0 \equiv r \pmod{24}$

donde r y todos los a_i's son conocidos excepto uno, sea a_j, en tal caso:

$$a_j 10^j \equiv r - \sum_{\substack{0 \le i \le 7 \\ i \ne j}} a_i 10^i \pmod{24}$$

Como 10 no es invertible mod. 24 (no son coprimos). la ecuación no tiene solución única, y por lo tanto no podemos averiguar a_j salvo que sea a_0 ($10^0 = 1$, que sí es invertible).

$\boxed{2.}$ Propiedad 1

Supongamos que en lugar de b_j, $1 \le j \le 10$, escribimos $b_j + e$ con $e \in \mathbb{Z}$, $-b_j \le e \le 9 - b_j$, no se detectará el error si:

$$-b_0 \equiv \sum_{1 \le i \le 10} b_i 10^{i-1} + e 10^{j-1} \pmod{12} \iff -b_0 \equiv -b_0 + e10^{j-1} \pmod{12} \iff$$

$$\iff e\, 10^{j-1} \equiv 0 \pmod{12}$$

Como antes, 10 y 12 no son coprimos, por lo que el error podría no detectarse. Por ejemplo, si $b_j = 2$ en la posición $j = 3$ (tercera posición) cometemos un error $e = 3$, este no se detectaría ya que $3 . 10^{3-1} = 3 . 10^2 = 300 \equiv 0 \pmod{12}$

Propiedad 2

Dados $b_0, b_1, \dots, b_{10}$ con $-b_0 \equiv \sum_{1\leq i\leq 10} b_i 10^{i-1} \pmod{12}$ permutamos b_j y b_{j+1}

No se detectará el error si $-b_0 \equiv \sum_{\substack{1\leq i\leq 10 \\ i\neq j}} b_i 10^{i-1} + b_j 10^{j-1} + b_{j+1} 10^{j} \pmod{12}$

$$-b_0 \equiv \sum_{1\leq i\leq 10} b_i 10^{i-1} + (b_j - b_{j+1})10^{j} + (b_{j+1} - b_j)10^{j-1} \pmod{12}$$

$$-b_0 \equiv -b_0 + 10^{j-1}\left((b_j - b_{j+1})10 + (b_{j+1} - b_j)\right) \pmod{12} \iff$$

$$\iff 0 \equiv 10^{j-1}(b_j - b_{j+1})(10-1) \pmod{12} \iff$$

$$\iff 9.10^{j-1}(b_j - b_{j+1}) \equiv 0 \pmod{12}$$

De nuevo, 9.10 no es coprimo con 12, no se tendrían por qué detectar ciertos errores.

Por ejemplo, error en la posición 2 y 3 ($j=2$) tal que $b_j - b_{j+1} = 2K$ $K \in \mathbb{N}$ ($b_j - b_{j+1}$ múltiplo de 2), entonces $9.10.2K = 180K \equiv 0 \pmod{12}$