1 Ejercicio 1

Propiedad 1: NO siempre se detecta un error

Al no ser 10 una unidad módulo 24, y al estar trabajando en un grupo finito, sabemos que 10 es un divisor de 0 (es decir, existe algún elemento $e \neq 0$ tal que $10^i e \equiv 0 \pmod{24}$ para cada uno de los valores de i salvo el 0). Sin embargo, puede que ese elemento e no esté entre los posibles valores que puede tomar en nuestro contexto del DNI, así que procedamos con más cuidado.

Veamos los valores de $10^i \pmod{24}$ para $i \in 0...7$ y sus correspondientes elementos de $\mathbb{Z}_{24}$ que al multiplicarlos entre sí nos dan 0 (si existiera, y si existe uno en el rango [-9,9], solo se tendrán en cuenta el resto de elementos que cumplan la ecuación en ese mismo rango):

$10^0 \equiv 1 \pmod{24} \rightarrow 1$ no es divisor de 0
$10^1 \equiv 10 \pmod{24} \rightarrow 10 \times \mathbf{12} \equiv 0 \pmod{24}$
$10^2 \equiv 4 \pmod{24} \rightarrow 4 \times \mathbf{6,\text{-}6} \equiv 0 \pmod{24}$
$10^3 \equiv 16 \pmod{24} \rightarrow 16 \times \mathbf{3,6,9,\text{-}3,\text{-}6,\text{-}9} \equiv 0 \pmod{24}$
$10^4 \equiv 16 \pmod{24} \rightarrow 16 \times \mathbf{3,6,9,\text{-}3,\text{-}6,\text{-}9} \equiv 0 \pmod{24}$
$10^5 \equiv 16 \pmod{24} \rightarrow 16 \times \mathbf{3,6,9,\text{-}3,\text{-}6,\text{-}9} \equiv 0 \pmod{24}$
$10^6 \equiv 16 \pmod{24} \rightarrow 16 \times \mathbf{3,6,9,\text{-}3,\text{-}6,\text{-}9} \equiv 0 \pmod{24}$
$10^7 \equiv 16 \pmod{24} \rightarrow 16 \times \mathbf{3,6,9,\text{-}3,\text{-}6,\text{-}9} \equiv 0 \pmod{24}$

Por tanto, y como 12 queda fuera del rango de valores que tenemos para los e, podríamos detectar los errores siempre y cuando los cometiéramos en la primera o segunda posición, o si los cometieramos en cualquier otra posición siempre y cuando no se dé la casualidad de que el error cometido sea de un múltiplo de 6 unidades en la tercera posición o de un múltiplo de 3 unidades de la tercera posición en adelante. Se añaden dos ejemplos en los que ilustramos casos en los que no podemos detectar el error, uno modificando la tercera cifra y otro la cuarta.

Ejemplos:

1.-
$11111011 \equiv 19 \pmod{24} \rightarrow$ Letra L
$11111611 \equiv 19 \pmod{24} \rightarrow$ Letra L

2.-
$11119111 \equiv 7 \pmod{24} \rightarrow$ Letra F
$11113111 \equiv 7 \pmod{24} \rightarrow$ Letra F

Propiedad 2: NO siempre se detecta la permutación de dos cifras consecutivas

Siguiendo los cálculos de las notas del curso, nos basta con encontrar para cada i un elemento $e \neq 0$ de $\mathbb{Z}_{24}$ tal que $10^i \times 9 \times e \equiv 0 \pmod{24}$. Procediendo de manera similar a la propiedad anterior, enumeraremos los valores de $10^i \times 9$ para $i \in 0...7$ y a su lado los números que multiplicados por él nos da 0 (si existieran, y si existe uno en el rango [-9,9], solo se tendrán en cuenta el resto de elementos que cumplan la ecuación en ese mismo rango):

$10^0 \times 9 \equiv 9 \pmod{24} \rightarrow 9 \times$ **8,-8** $\equiv 0 \pmod{24}$
$10^1 \times 9 \equiv 18 \pmod{24} \rightarrow 18 \times$ **4,8,-4,-8** $\equiv 0 \pmod{24}$
$10^2 \times 9 \equiv 12 \pmod{24} \rightarrow 12 \times$ **2,4,6,8,-2,-4,-6,-8** $\equiv 0 \pmod{24}$
$10^3 \times 9 \equiv 0 \pmod{24} \rightarrow$ Ya tenemos directamente 0 sin importar el valor de e
$10^4 \times 9 \equiv 0 \pmod{24} \rightarrow$ Ya tenemos directamente 0 sin importar el valor de e
$10^5 \times 9 \equiv 0 \pmod{24} \rightarrow$ Ya tenemos directamente 0 sin importar el valor de e
$10^6 \times 9 \equiv 0 \pmod{24} \rightarrow$ Ya tenemos directamente 0 sin importar el valor de e
$10^7 \times 9 \equiv 0 \pmod{24} \rightarrow$ Ya tenemos directamente 0 sin importar el valor de e

Por lo tanto, podremos detectar el error si la permutación se da entre la primera y segunda posición, entre la segunda y la tercera o entre la tercera y la cuarta, siempre y cuando la diferencia entre los dígitos a permutar no sea múltiplo de 8 en el primer caso, múltiplo de 4 en el segundo y múltiplo de 2 en el tercero. En el resto de permutaciones no podremos detectar el error sin importar los dígitos que ocupen los respectivos lugares.

Ejemplos:

1.-
$11111119 \equiv 7 \pmod{24} \rightarrow$ Letra F
$11111191 \equiv 7 \pmod{24} \rightarrow$ Letra F

2.-
$98111111 \equiv 23 \pmod{24} \rightarrow$ Letra Ñ
$89111111 \equiv 23 \pmod{24} \rightarrow$ Letra Ñ

Propiedad 4: Nunca se puede corregir un error aunque sepamos la posición donde se ha producido

En los casos en los que no podemos detectar el error es evidente que mucho menos podremos arreglarlo. En el caso de que desconozcamos la primera cifra por la derecha, al ser $10^0 = 1$ y $mcd(1, 24) = 1$ tenemos que esa ecuación (la que aparece en la propiedad 4 de las notas del curso) tiene solución única y, por tanto, podremos obtener el valor original del primer dígito. Para el resto de casos tenemos que resolver la misma ecuación, pero en este caso 10 no es coprimo con 24, por lo que al ser una ecuación lineal, usando el teorema chino del resto y sabiendo que $mcd(10^i, 24) \neq 1 \ \forall i \in 1...7$, tenemos que esa ecuación tendrá o bien ninguna o bien más de una solución, por lo que no podemos obtener el valor original.

2 Ejercicio 2

Propiedad 1: NO siempre se puede detectar un error

En base a los cálculos de la propiedad 1 del CCC de las notas del curso, nos basta con analizar si la ecuación $e10^{j-1} \equiv 0 \pmod{12}$ tiene solución no trivial. Como en el ejercicio anterior, ahora 10 no es invertible módulo 12 y, por tanto, es divisor de 0. Procedamos enumerando los números que multiplicados por cada 10^{j-1} nos dan 0:

$10^0 \equiv 1 \pmod{12} \rightarrow 1$ no es divisor de 0
$10^1 \equiv 10 \pmod{12} \rightarrow 10 \times \mathbf{6} \equiv 0 \pmod{12}$
$10^2 \equiv 4 \pmod{12} \rightarrow 4 \times \mathbf{3{,}6{,}9} \equiv 0 \pmod{12}$
$10^3 \equiv 4 \pmod{12} \rightarrow 4 \times \mathbf{3{,}6{,}9} \equiv 0 \pmod{12}$
$10^4 \equiv 4 \pmod{12} \rightarrow 4 \times \mathbf{3{,}6{,}9} \equiv 0 \pmod{12}$
$10^5 \equiv 4 \pmod{12} \rightarrow 4 \times \mathbf{3{,}6{,}9} \equiv 0 \pmod{12}$
$10^6 \equiv 4 \pmod{12} \rightarrow 4 \times \mathbf{3{,}6{,}9} \equiv 0 \pmod{12}$
$10^7 \equiv 4 \pmod{12} \rightarrow 4 \times \mathbf{3{,}6{,}9} \equiv 0 \pmod{12}$
$10^8 \equiv 4 \pmod{12} \rightarrow 4 \times \mathbf{3{,}6{,}9} \equiv 0 \pmod{12}$
$10^9 \equiv 4 \pmod{12} \rightarrow 4 \times \mathbf{3{,}6{,}9} \equiv 0 \pmod{12}$

Por tanto, si cometemos el error en el dígito b_1 detectaremos el error, pero en el resto de los casos solo lo detectaremos si el error en la segunda posición es distinto de 6 o en el resto de posiciones si el error cometido no es múltiplo de 3.

Ejemplos (Escribimos el número de la forma en la que aparece en los apuntes, para realizar el cálculo del módulo hay que darle la vuelta antes):

1.-
$1111111111 \equiv 7 \pmod{12}$
$1711111111 \equiv 7 \pmod{12}$

2.-
$9999999999 \equiv 3 \pmod{12}$
$9999999993 \equiv 3 \pmod{12}$

Propiedad 2: NO siempre se puede detectar una permutación de dos dígitos consecutivos

Siguiendo el desarrollo de la propiedad de las notas, podemos usar los mismos cálculos hasta obtener la ecuación $9 \times 10^{j-1}(b_j - b_{j+1}) \equiv 0 \pmod{12}$, aunque ahora no podemos llegar a la conclusión de que $(b_j - b_{j+1})$ sea congruente con 0 módulo 12 ya que ni 9 ni 10 son coprimos con 12, y, por tanto, no son invertibles módulo 12. Para analizar cada situación, calculamos los valores de $9 \times 10^{j-1}$ (mod 12) para los valores de j de 0 a 9 y los elementos de $\mathbb{Z}_{12}$ que al multiplicarlos por esa expresión nos da 0 (Solo se incluyen los elementos que tienen sentido dentro de que los b_i):

$9 \times 10^0 \equiv 9 \pmod{12} \rightarrow 9 \times \mathbf{4,8} \equiv 0 \pmod{12}$
$9 \times 10^1 \equiv 6 \pmod{12} \rightarrow 6 \times \mathbf{2,4,6,\text{-}2,\text{-}4} \equiv 0 \pmod{12}$
$9 \times 10^2 \equiv 0 \pmod{12} \rightarrow$ Ya tenemos directamente 0
$9 \times 10^3 \equiv 0 \pmod{12} \rightarrow$ Ya tenemos directamente 0
$9 \times 10^4 \equiv 0 \pmod{12} \rightarrow$ Ya tenemos directamente 0
$9 \times 10^5 \equiv 0 \pmod{12} \rightarrow$ Ya tenemos directamente 0
$9 \times 10^6 \equiv 0 \pmod{12} \rightarrow$ Ya tenemos directamente 0
$9 \times 10^7 \equiv 0 \pmod{12} \rightarrow$ Ya tenemos directamente 0
$9 \times 10^8 \equiv 0 \pmod{12} \rightarrow$ Ya tenemos directamente 0
$9 \times 10^9 \equiv 0 \pmod{12} \rightarrow$ Ya tenemos directamente 0

Por tanto, y como hemos procedido en apartados anteriores, podremos detectar la permutación de dos dígitos contiguos siempre y cuando la diferencia entre ellos no sea múltiplo de 4 cuando se hayan permutado las dos primeras cifras o no sea múltiplo de 2 cuando se hayan permutado la segunda y la tercera cifra. En cualquier otro caso, no nos es posible detectar esa permutación.

Ejemplos (Escribimos el número de la forma en la que aparece en los apuntes, para realizar el cálculo del módulo hay que darle la vuelta antes):

1.-
$9111111111 \equiv 3 \pmod{12}$
$1911111111 \equiv 3 \pmod{12}$

2.-
$1234567891 \equiv 1 \pmod{12}$
$1234657891 \equiv 1 \pmod{12}$