Códigos detectores de errores.

El NIF

El NIF consta de 8 números (DNI) y una letra. Para asignarle la letra al DNI se toma el resto módulo 23 y se utiliza la siguiente tabla.

0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
T	R	W	A	G	M	Y	F	P	D	X	B

12	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**
N	J	Z	S	Q	V	H	L	C	K	E

Por ejemplo, al DNI 01234567 le corresponde la letra L pues $01234567 = 23 \times 53676 + 19$ o, lo que es lo mismo, $1234567 \equiv 19 (\text{mod } 23)$.

La asignación de esas letras a cada resto es arbitraria.

Dado un DNI digamos N, si escribiéramos el DNI con errores N_e, no se detectarían los errores si a ambos números les correspondiera la misma letra, es decir, si fueran congruentes módulo 23.

1 El NIF detecta siempre un error.

Demostración:

Escribamos el número de 8 cifras 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 $0 \leqslant a_i \leqslant 9$ y 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 $(a_i + e)$, $e \in \mathbb{Z}$ y $-a_i \leqslant e \leqslant 9 - a_i$.

Llamemos N_e al número 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 la letra asignada a ambos números fuera la misma, es decir, si tuvieran el mismo resto módulo 23:

$N \equiv N + e\ 10^i\ (mod\ 23) \Leftrightarrow e\ 10^i \equiv 0 \ (\text{mod } 23) \Leftrightarrow e \equiv 0 \ (\text{mod } 23) \Leftrightarrow e = 0$. Por tanto, las letras solo serán iguales si el error cometido es 0, es decir, si no se ha cometido ningún error. Por tanto si se ha cometido un único error el resto módulo 23 ha cambiado.

2 El NIF detecta siempre una permutación de dos cifras consecutivas (un error muy común)

Demostración:

Supongamos que se han permutado las cifras que ocupan las posiciones i e $i+1$, $0 \leqslant i \leqslant 6$. Para no detectar el error, las letras asignadas a ambos números tendrían que se la misma, es decir

$N \equiv N_e \ (\text{mod } 23) \Leftrightarrow N - N_e \equiv 0 \ (\text{mod } 23)$.

$N - N_e = (a_{i+1} - a_i)\ 10^{i+1} + (a_i - a_{i+1})\ 10^i = (a_{i+1} - a_i)\ 10^i \cdot 9 \equiv 0 \ (\text{mod } 23) \Leftrightarrow (a_{i+1} - a_i) \equiv 0 \ (\text{mod } 23)$.

Como $a_{i+1} - a_i$ es un número entero entre -9 y 9, $(a_{i+1} - a_i) \equiv 0 \ (\text{mod } 23) \Leftrightarrow a_{i+1} - a_i = 0$, es decir, si las dos cifras permutadas eran iguales y, por lo tanto, no se ha cometido ningún error.

3 El NIF no siempre detecta dos errores cualesquiera

Demostración:

Supongamos que se han cometido errores e_i y e_j en las posiciones i y j con $i > j$.

No detectaríamos el error si la letra asignada a ambos números fuera la misma, es decir, si $N \equiv N_e$ (mod 23).

$N_e - N = e_i\ 10^i + e_j\ 10^j = 10^j(e_i\ 10^{i-j} + e_j) \equiv e_i\ 10^{i-j} + e_j \equiv 0 \ (\text{mod } 23)$.

Y esta ecuación tiene soluciones no triviales.

Por ejemplo, $5 \times 10^4 + 2$ es solución, pues $50002 = 23 \times 2.174$. Esto significa que si, por ejemplo, en lugar de escribir 3**4**012**6**49L escribiéramos 3**9**012**8**49L (dos errores separados 4 unidades, el primero $e_6 = 5$ y el segundo $e_2 = 2$), no se detectaría ningún error pues a ambos DNI les corresponde la letra L.

Dados i, j y e_i, la tabla muestra los valores que debe tomar e_j para que $e_i\ 10^{i-j} + e_j \equiv 0 \pmod{23}$.

i-j / e_i	**-9**	**-8**	**-7**	**-6**	**-5**	**-4**	**-3**	**-2**	**-1**	**~~0~~**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
1	-2	~~11~~	1	-9	4	-6	7	-3	~~10~~	~~0~~	~~13~~	3	-7	6	-4	9	-1	~~12~~	2
2	3	-5	~~10~~	2	-6	9	1	-7	8	~~0~~	-8	7	-1	-9	6	-2	~~13~~	5	-3
3	7	-4	8	-3	9	-2	~~10~~	-1	~~11~~	~~0~~	~~12~~	1	~~13~~	2	-9	3	-8	4	-7
4	1	6	~~11~~	-7	-2	3	8	~~13~~	-5	~~0~~	5	~~10~~	-8	-3	2	7	~~12~~	-6	-1
5	~~10~~	-9	-5	-1	3	7	~~11~~	-8	-4	~~0~~	4	8	~~12~~	-7	-3	1	5	9	~~13~~
6	8	2	-4	~~13~~	7	1	-5	~~12~~	6	~~0~~	-6	~~11~~	5	-1	-7	~~10~~	4	-2	-8
7	~~11~~	-3	6	-8	1	~~10~~	-4	5	-9	~~0~~	9	-5	4	~~13~~	-1	8	-6	3	~~12~~

4 El NIF se puede usar para corregir un error siempre que se sepamos cuál es su posición.
Supongamos que la cifra que está en la posición i es ilegible, pero conocemos las 7 cifras restantes y la letra (es decir, el resto módulo 23 del DNI).

Tenemos, $N = a_7 10^7 + a_6 10^6 + a_5 10^5 + a_4 10^4 + a_3 10^3 + a_2 10^2 + a_1 10 + a_0 \equiv r \pmod{23}$,
donde r y todos los a_i son conocidos salvo uno, sea a_j, en tal caso
$a_j 10^j \equiv r - \sum_{0 \leqslant i \leqslant 7\ (i \neq j)} a_i \times 10^i \pmod{23}$
Al ser 10 invertible módulo 23, la ecuación tiene solución única y, por tanto, podemos saber qué cifra es la borrada.

Así pues, el NIF puede usarse para detectar un error, no siempre detecta dos errores, pero sí detecta la permutación de dos cifras consecutivas. Además, puede usarse para corregir un error siempre que se sepa en que posición está.

Código Cuenta Cliente (CCC)
Un número de cuenta bancaria consta de 20 cifras.

$$a_3a_4a_5a_6 \quad a_7a_8a_9a_{10} \quad A_0B_0 \quad b_1b_2b_3b_4b_5b_6b_7b_8b_9b_{10}$$

- Cuatro cifras para la Entidad
- Cuatro para la Oficina
- Dos para los dígitos de control (DC)
- Diez cifras finales para el número de cuenta del cliente.

Dados a_i y b_i (con índices no nulos) para asignar A_0 y B_0 calculamos a_0 y b_0 de manera que se cumplan las siguientes igualdades:

$$-a_0 \equiv a_3 10^2 + a_4 10^3 + a_5 10^4 + a_6 10^5 + a_7 10^6 + a_8 10^7 + a_9 10^8 + a_{10} 10^9 \ (mod\ 11)$$
$$-b_0 \equiv b_1 10^0 + b_2 10^1 + b_3 10^2 + b_4 10^3 + b_5 10^4 + b_6 10^5 + b_7 10^6 + b_8 10^7 + b_9 10^8 + b_{10} 10^9 \ (mod\ 11)$$

Si $a_0 \neq 10$ entonces $A_0 = a_0$, pero si $a_0 = 10$ entonces $A_0 = 1$ lo que crea ambigüedad. Lo mismo para B_0.

Observa que el primer dígito de control solo depende de las 8 cifras iniciales y el segundo de las 10 últimas. Además se observa que la primera fórmula es un caso particular de la segunda con $b_1 = b_2 = 0$. Estudiaremos la segunda ecuación por ser más general.

Notemos que
$$-b_0 \equiv \sum_{1 \leqslant i \leqslant 10} b_i\ 10^{i-1} \ (mod\ 11)$$

1 El CCC detecta siempre un error (siempre que el dígito de control B_0 no sea 1).

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

$$-b_0 \equiv \sum_{1\leqslant i\leqslant 10} b_i\ 10^{i-1} + e\ 10^{j-1}\ (mod\ 11)$$

$$\Leftrightarrow -b_0 \equiv -b_0 + e\ 10^{j-1}\ (mod\ 11) \Leftrightarrow 0 \equiv e\ 10^{j-1}\ (mod\ 11) \Leftrightarrow e = 0$$

.

Por tanto, si se comete un error el valor de b_0 cambia y si $B_0 \neq 1$ se detecta que hay un error.

¿Qué puede ocurrir si $B_0 = 1$?

Supongamos, por ejemplo que $b_0 = 1$, o sea

$$-1 \equiv \sum_{1\leqslant i\leqslant 10} b_i\ 10^{i-1}\ (mod\ 11)$$

nos preguntamos si existen j y e (no nulo) de modo que

$$-10 \equiv \sum_{1\leqslant i\leqslant 10} b_i\ 10^{i-1} + e\ 10^{j-1}\ (mod\ 11)$$

Esto equivale a

$$-10 \equiv -1 + e\ 10^{j-1}$$

que admite solución no trivial e.

Así pues, si el dígito de control es 1, es posible no detectar un error.

Por ejemplo el número de cuenta 3333333334 tiene dígito de control 1 y 3333333332 también (en la primera $b_0 = 1$ y en la segunda $b_0 = 10$.

EN GENERAL

Ya hemos visto que la ecuación

$$-b_0 \equiv \sum_{1\leqslant i\leqslant 10} b_i\ 10^{i-1} + e\ 10^{j-1}\ (mod\ 11)$$

tiene solución única $e = 0$. Nos preguntamos si la ecuación

$$b_0 - 11 \equiv \sum_{1\leqslant i\leqslant 10} b_i\ 10^{i-1} + e\ 10^{j-1}\ (mod\ 11)$$

tiene soluciones no triviales ya que, si $b_0 = 1$ o si $b_0 = 10$ la cuenta inicial y la cuenta con error tendrán el mismo $B_0 = 1$ y no se detectaría el error.

$$b_0 - 11 \equiv \sum_{1\leqslant i\leqslant 10} b_i\ 10^{i-1} + e\ 10^{j-1}\ (mod\ 11)$$

$$\Leftrightarrow b_0 - 11 \equiv -b_0 + e\ 10^{j-1}\ (mod\ 11) \Leftrightarrow 2b_0 \equiv e\ 10^{j-1}\ (mod\ 11)$$

que tiene tiene solución

$e = 2$ si $b_0 = 1$ y j impar o si $b_0 = 10$ y j par

$e = 9$ si $b_0 = 1$ y j par o si $b_0 = 10$ y j impar

2 El CCC detecta siempre una permutación de dos dígitos consecutivos (siempre que el dígito de control no sea 1).

Dados $b_0\ b_1 \ldots b_{10}$ con

$$-b_0 \equiv \sum_{1\leqslant i\leqslant 10} b_i\ 10^{i-1}\ (mod\ 11)$$

permutamos b_j y b_{j+1}. No se detectará el error si

$$-b_0 \equiv \sum_{1\leqslant i\leqslant 10\ \ i\neq j,j+1} b_i 10^{i-1} + b_j 10^j + b_{j+1}10^{j-1}\ (mod\ 11)$$
$$-b_0 \equiv \sum_{1\leqslant i\leqslant 10} b_i 10^{i-1} + (b_j - b_{j+1})10^j + (b_{j+1} - b_j)10^{j-1}\ (mod\ 11)$$

$$-b_0 \equiv -b_0 + 10^{j-1}((b_j - b_{j+1})10 + (b_{j+1} - b_j))\ (mod\ 11) \Leftrightarrow 0 \equiv 10^{j-1}(b_j - b_{j+1}) \times (10-1)\ (mod\ 11)$$

$$\Leftrightarrow 0 \equiv (b_j - b_{j+1})\ (mod\ 11) \Leftrightarrow b_j = b_{j+1}$$

Así pues, si $B_0 \neq 1$ siempre se detectará una permutación de dos cifras consecutivas.

¿Qué ocurre si $B_0 = 1$?

Supongamos que $b_0 = 1$ y

$$-1 \equiv \sum_{1\leqslant i\leqslant 10} b_i 10^{i-1}\ (mod\ 11)$$

Nos plantemos si la ecuación

$$-10 \equiv \sum_{1\leqslant i\leqslant 10\ \ i\neq j,j+1} b_i 10^{i-1} + b_j 10^j + b_{j+1}10^{j-1}\ (mod\ 11)$$

tiene solución.

$$-10 \equiv \sum_{1\leqslant i\leqslant 10} b_i 10^{i-1} + (b_j - b_{j+1})10^j + (b_{j+1} - b_j 10^{j-1})\ (mod\ 11)$$
$$-10 \equiv -1 + (b_j - b_{j+1})(10^j - 10^{j-1})\ (mod\ 11)$$
$$-9 \equiv 9 \times 10^{j-1} \times (b_j - b_{j+1})\ (mod\ 11)$$
$$(-1)^j \equiv b_j - b_{j+1}\ (mod\ 11)$$

que tiene tiene solucíon con $b_j \neq b_{j+1}$.

Por ejemplo, para $j = 3$, $b_j = 3$ y $b_{j+1} = 4$

Los números de cuenta 1234567896 y 1243567896 tienen ambos $B_0 = 1$, en el primero $b_0 = 1$ y en el segundo $b_0 = 10$.

3 El CCC no siempre detecta dos errores

Supongamos que cometemos errores e_j y e_k, es decir, remplazamos las cifras b_j y b_k por $b_j + e_j$ y $b_k + e_k$ con $1 \leqslant j \leqslant k \leqslant 10$.

Dados los b_i con

$$-b_0 \equiv \sum_{1\leqslant i\leqslant 10} b_i 10^{i-1}\ (mod\ 11)$$

La ecuación

$$-b_0 \equiv \sum_{1\leqslant i\leqslant 10} b_i 10^{i-1} + e_j 10^{j-1} + e_k 10^{k-1}\ (mod\ 11)$$
$$0 \equiv e_j 10^{j-1} + e_k 10^{k-1}\ (mod\ 11)$$

puede tener soluciones no triviales.

Por ejemplo, 0123456789 y 0128450789 tienen ambas $B_0 = 5$

4 El CCC puede utilizarse para corregir un error si se conoce su posición (siempre que el dígito de control no sea 1)

Supongamos que sabe que en la posición j hay un error. Debemos encontrar x que satisfaga la ecuación

$$-b_0 \equiv \sum_{1\leqslant i\leqslant 10\ \ i\neq j} b_i 10^{i-1} + x10^{j-1}\ (mod\ 11)$$
$$x10^{j-1} \equiv -b_0 - \sum_{1\leqslant i\leqslant 10\ \ i\neq j} b_i 10^{i-1}\ (mod\ 11)$$

que tiene solución única al ser 10 invertible módulo 11.

Si $B_0 = 1$ ya vimos que no se detectaba un error, por lo que no se puede utilizar para corregir errores.

Problemas

1) Modificamos el código detector de errores del NIF agregando la letra Ñ, que ponemos en correspondencia con el número 23, y reemplazamos el módulo 23 por el módulo 24. Analiza las propiedades 1), 2) y 4) para el código corrector definido en esta nueva forma.

2) Definamos ahora una modificación de CCC considerando $B_0 = b_0$ en todos los casos (incluso si b_0 tiene dos cifras), pero ahora

$$-b_0 \equiv \sum_{1 \leqslant i \leqslant 10} b_i \ 10^{i-1} \ (mod\ 12)$$

(en lugar de módulo 11). Analiza las propiedades 1), 2) en esta nueva definición.