PROBLEMAS

1

Añadimos la $\bar{N} \to 23$

Propiedad 1: El NIF detecta siempre un error.

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

$$N_e = N + e \cdot 10^i$$

- No se detecta error si $N \equiv N_e \pmod{24}$

$$N \equiv N + e \cdot 10^i \pmod{24}$$

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

$$0 \equiv e \cdot 5^i \cdot 2^i \pmod{24}$$

- Tiene más de una solución además de $e=0$. Por ejemplo, si $e=3$, $i=3$.

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

$$N_e = a_7 \cdot 10^7 + a_6 \cdot 10^6 + a_5 \cdot 10^5 + a_4 \cdot 10^4 + \boxed{(a_3 + 3)} \cdot 10^3 + a_2 + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$$

- Comprobamos si se cumple:

$$N \equiv N_e \pmod{24}$$

$$N \equiv N + 3 \cdot 10^3 \pmod{24}$$

$$0 \equiv 3 \cdot 2^3 \cdot 5^3 \pmod{24}$$

$$0 \equiv 24 \cdot 5^3 \pmod{24}$$

- Como, evidentemente, $24 \cdot 5^3$ es divisible entre 24, $N \equiv N_e \pmod{24}$ para un $e \neq 0$.

$$\boxed{\text{NO SE CUMPLE LA PROPIEDAD}}$$

Propiedad 2: El NIF siempre detecta una permutación de dos cifras.

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

$$= (a_i - a_{i+1} + 10 \cdot a_{i+1} - 10 \cdot a_i) \cdot 10^i \pmod{24}$$

$$= 9 \cdot (a_{i+1} - a_i) \cdot 2^i \cdot 5^i \pmod{24}$$

$$= 3 \cdot 2^i \cdot (a_{i+1} - a_i) \cdot 5^i \pmod{24}$$

- Esto es congruente con 0 módulo 24 para varias soluciones, de hecho, independientes de los valores a_i, a_{i+1}.
- Por ejemplo, bastaría con intercambiar el número de las posiciones 3 y 4.

  $N = 05303839 = 220993 \cdot 24 + 7$

  $N_e = 05330839 = 222118 \cdot 24 + 7$

$$\boxed{\text{NO SE CUMPLE LA PROPIEDAD}}$$

Propiedad 4: El NIF puede corregir un error siempre que sepamos cuál es su posición.

- Suponemos que a_i, $i \neq j$ conocidos y que $\sum_{i=0}^{7} a_i \cdot 10^i \equiv r \pmod{24}$ a_j desconocido.
- Por tanto:

$$a_j \cdot 10^j \equiv r - \sum_{\substack{i=0 \\ i \neq j}}^{7} a_i \cdot 10^i \pmod{24}$$

- Como $(10, 24) = 2 \neq 1 \Rightarrow 10$ no es invertible módulo 24 y por tanto, de haber solución, no sería única y no se podría corregir con certeza.

$$\boxed{\text{NO SE CUMPLE LA PROPIEDAD}}$$

(2)

$B_0 = b_0$

$$-b_0 \equiv \sum_{i=1}^{10} b_i \cdot 10^{i-1} \pmod{12}$$

Antes:

$$-b_0 \equiv \sum_{i=1}^{10} b_i \cdot 10^{i} \pmod{11}$$

$B_0 = b_0$ si $b_0 \neq 10$

$B_0 = 1$ si $b_0 = 1$

Propiedad 1: El CCC detecta siempre un error.

- No se detectará error si:

$$-b_0 \equiv \left(\sum_{i=1}^{10} b_i \cdot 10^{i-1}\right) + e \cdot 10^{j-1} \pmod{12}$$

$$-b_0 \equiv -b_0 + e \cdot 10^{j-1} \pmod{12}$$

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

$$0 \equiv e \cdot 2^{j-1} \cdot 5^{j-1} \pmod{12}$$

- No se detecta error si, por ejemplo, $e = 3$ y $j = 3$.

$$0 \equiv 3 \cdot 2^2 \cdot 5^2 \pmod{12}$$

$$0 \equiv 12 \cdot 5^2 \pmod{12}$$

NO SE CUMPLE LA PROPIEDAD

Propiedad 2: El CCC detecta siempre una permutación de dos dígitos consecutivos

• No se detecta el error si:

$$-b_0 \equiv \sum_{i=1}^{10} b_i \cdot 10^{i-1} \pmod{12} \equiv \sum_{\substack{i=1 \\ i\neq j,j+1}}^{10} b_i \cdot 10^{i-1} + b_j \cdot 10^{j} + b_{j+1} \cdot 10^{j-1} \pmod{12}$$

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

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

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

$$0 \equiv 9 \cdot 10^{j-1} \cdot b_j - 9 \cdot 10^{j-1} \pmod{12}$$

• Como $12 = 2^2 \cdot 3$, basta con que $j \geq 3$ para que el código no detecte error, independientemente de los valores de b_j y b_{j+1}. Por ejemplo:

Correcto → 112 3 2 5 6 8 9 7 $\quad b_5 = 2$

Incorrecto → 1 1 2 3 5 2 6 8 9 7 $\quad b_6 = 5$

$1123256897 = 93604741 \cdot 12 + 5 \equiv 5 \pmod{12}$

$1123526897 = 93.627.241 \cdot 12 + 5 \equiv 5 \pmod{12}$

$\boxed{\text{NO SE CUMPLE LA PROPIEDAD}}$