Sea $n$ un número entero positivo, y sea $\mathbb{Z}_n$ el anillo de enteros módulo $n$. Supóngase que existe una función $f : \mathbb{Z}_n \to \mathbb{Z}_n$ que satisface las siguientes propiedades:

1. $f(x) \neq x$,
2. $f(f(x)) = x$,
3. $f(f(f(x+1)+1)+1) = x$, para todo $x \in \mathbb{Z}_n$

Prueba que $n \equiv 2 \pmod 4$.

**Solución:**

En primer lugar, se ve que $f$ es una permutación sobre los elementos de $\mathbb{Z}_n$, sin ningún punto fijo, por la primera propiedad.

Una permutación se puede descomponer en un producto de transposiciones. En este caso, las transposiciones de la permutación $f$ son de la forma $(x, f(x))$, de manera que $f \circ f$ es la identidad. Por este motivo, las transposiciones son disjuntas, lo cual indica que el número de transposiciones es $\frac{n}{2}$ y por tanto $n$ es un número par.

Sea $g(x) = f(x+1)$. Si $g$ fuera una permutación impar, entonces $g \circ g \circ g$ es impar, pero $g(g(g(x))) = g(g(f(x+1))) = g(f(f(x+1)+1)) = f(f(f(x+1)+1)+1) = x$, por la tercera propiedad de $f$. Como la permutación identidad es par, se contradice que $g$ es impar, por lo que $g$ es par.

Considerando la permutación cíclica $h(x) = x - 1$, esta es impar porque el número de elementos no fijos es $n$, que es un número par.

Entonces, $f = g \circ h$ es una permutación impar, lo cual implica que el número de transposiciones en las que se puede descomponer la permutación es impar, es decir, que $\frac{n}{2}$ es impar. Finalmente, esto es lo mismo que decir que $n \equiv 2 \pmod 4$.