P3a. Como n es divisor de m, tenemos que existe p natural tal que $m = np$. Entonces

$$z^m = (z^n)^p = 1^p = 1$$

donde utilizamos que z es raíz n-ésima de la unidad.

P3b. Observemos primero que $U \neq \emptyset$, ya que $1^n = 1$ para cualquier $n \geq 2$. Entonces, dados $z, w \in U$, debemos demostrar que $z \cdot w^{-1} \in U$. Es decir, que $z \cdot w^{-1}$ es raíz n-ésima de la unidad para algún $n \geq 2$.

Como $z, w \in U$, sean $p, q \geq 2$ tales que z es raíz p-ésima y w es raíz q-ésima de la unidad.

Opción 1: Usando la parte anterior, obtenemos que tanto z como w son raíces $(p \cdot q)$-ésimas de la unidad, y por lo tanto también lo es $z \cdot w^{-1}$.

Opción 2: Se puede calcular directamente:

$$(z \cdot w^{-1})^{p \cdot q} = \frac{z^{p \cdot q}}{w^{p \cdot q}} = \frac{(z^p)^q}{(w^q)^p} = \frac{1^q}{1^p} = 1$$

Basta finalmente notar que $p \cdot q \geq 4 \geq 2$, y concluimos que $(U, \cdot)$ es subgrupo de $(S, \cdot)$.

Pextra1. Notemos que las potencias de w: $w, w^2, w^3, w^4, w^5, \ldots$ forman una secuencia infinita. Como W es grupo, todas estas potencias pertenecen a W, el cual es un conjunto de n elementos. Por lo tanto, la secuencia debe repetirse en algún momento. Es decir, deben existir un j y un $l > j$ tales que $w^l = w^j$. Entonces $w^m = 1$, tomando $m = l - j$. Considerando que W tiene sólo n elementos, este m debe valer a lo más n.

Pextra2. Siguiendo un argumento similar al de la parte anterior: si W' tuviera menos de m elementos, entonces existirían $j, l \in \{0, 1, \ldots, m-1\}$ tales que $l > j$ y $w^j = w^l$. Entonces, llamando $p = l - j$, tenemos que $w^p = 1$ y $p = l - j \leq (m-1) - 0 < m$, lo que contradice que m es el menor exponente posible.

Para lo siguiente: W' es no vacío pues $1 \in W'$. Además, si tomamos w^p y w^q elementos de W', entonces

$$w^p \cdot (w^q)^{-1} = w^{p-q}$$

Caso 1: $p \geq q$. Se tiene que $0 \leq p - q \leq m - 1$, por lo tanto $w^{p-q} \in W'$.

Caso 2: $p < q$. En este caso, observamos que $q - p \leq m$, y escribimos

$$w^{p-q} = 1 \cdot w^{p-q} = w^m \cdot w^{p-q} = w^{m-(q-p)}$$

Notando que $0 \leq m - (q - p) \leq m - 1$, obtenemos para este otro caso que también $w^{p-q} \in W'$.

Concluimos, entonces, que W' es subgrupo de W.

Pextra3. El Teorema de Lagrange dice que el orden de todo subgrupo de un grupo finito divide al orden del grupo, por lo que obtenemos que $|W'|$ divide a $|W|$, es decir que m divide a n.

Por lo tanto, tenemos que $n = k \cdot m$ para algún k natural, y entonces $z^n = z^{k \cdot m} = (z^m)^k = 1$.

La conclusión final: Hemos demostrado en las etapas anteriores que todos los elementos de W son raíces n-ésimas de la unidad. Como W tiene n elementos, éstos deben ser exactamente las n raíces n-ésimas.