Si G es un grupo que no tiene subgrupos no triviales (solo tiene subgrupos triviales), demostrar que G es finito de orden primo.

Dem.

Primero se demuestra un resultado que nos es útil para probar que es finito cíclico.

1. Sea G un grupo cíclico finito de orden n ($a \in G$ tal que $G = \langle a \rangle$). Demostrar que para cada divisor d de n, G contiene un único subgrupo de orden d.

Dem.

Sea $a^{\frac{n}{d}} \in G$ cuyo orden es d

dado que $(a^{\frac{n}{d}})^d = a^n = e$.

Sea $H = \langle a^{\frac{n}{d}} \rangle$ entonces $|H| = d$.

Sea $H_1 < G$ tal que $|H_1| = d$.

H_1 es cíclico, sea $c \in H_1$ tal que $H_1 = \langle c \rangle$.

Como $H_1 \in G = \langle a \rangle$,

c se puede expresar de la siguiente manera

$c = a^m, m \in \mathbb{Z}$.

Entonces $e = c^d = (a^m)^d \Rightarrow n | md$ *

luego $md = nt, t \in \mathbb{Z}$

$\Rightarrow m = (\frac{n}{d})t \Rightarrow c = a^m = (a^{\frac{n}{d}})^t \in \langle a^{\frac{n}{d}} \rangle = H$.

Por lo tanto $H_1 = \langle c \rangle \subseteq H$, pero $|H| = d = |H_1|$

Por lo tanto $H = H_1$

* tengo dudas respecto a como hacen la comparación para determinar que $n | md$ con el resultado anterior $e = c^d = (a^m)^d = a^n$, yo supongo (no estoy convencido al 100%) que también se cumple $md | n$, pero se toma el anterior porque nos lleva al resultado de una forma más elegante.

Ahora demostrar que es finito.

Supongamos que G *no es un grupo cíclico*.

Por la negación de 1 tenemos que para

$d \| G |, con\ d \in \mathbb{Z}$

existen al menos $H_1, H_2 < G$
$H_1 \neq H_2 \; y \; |H_1| = d = |H_2|$

H_1 solo puede ser $\{e\}$ o G.
H_2 solo puede ser $\{e\}$ o G.

Si $H_1 = e = H_2 \Rightarrow H_1 = H_2$ (contradicción).
Si $H_1 = G = H_2 \Rightarrow H_1 = H_2$ (contradicción).

Por lo tanto G es cíclico finito.

Ahora el final de esto (que es de orden primo).

Sea $|G| = n$, suponer que n no es primo.

Entonces existe $d \in \mathbb{Z}$
tal que $d|n, d > 1 \; y \; d < n$,

entonces existe $H < G$ (único) tal que $|H| = d$.

Sí $H = \{e\} \Rightarrow |H| = 1$ (contradicción).
Sí $H = G \Rightarrow |H| = n$ (contradicción).

Por lo tanto n es primo.