$g \in G$ d'ordre n

Montrer $\langle g \rangle$ de cardinal n et

$$\langle g \rangle = \{g^0, \dots, g^{n-1}\}$$

On a $\langle g \rangle = \{g^t : t \in \mathbb{Z}\}$

Soit $t \in \mathbb{Z}$, div. euclidienne $t = nq + r$

avec $0 \leq r \leq n-1$ alors $g^t = (\underbrace{g^n}_{e})^q \cdot g^r = g^r$

d'où $\langle g \rangle = \{g^r : 0 \leq r \leq n-1\}$

Il reste à montrer que tous les g^r pour $0 \leq r \leq n-1$ sont distincts.

Supposons $g^r = g^s$ avec $0 \leq s < r \leq n-1$

alors $g^{r-s} = e$ avec $0 < r-s \leq n-1 < n$

impossible car n est l'ordre de g.