**Thm** (Fundamental Theorem of Cyclic Groups) FTCG

Consider a cyclic group. Let $a$ be a generator of the group. (Thus the group can be expressed $\langle a \rangle$.)

1. Every subgroup of a cyclic group is cyclic.
2. If $\langle a \rangle$ has order $n$, the order of every subgroup of $\langle a \rangle$ is a divisor of $n$.
3. For each divisor $d$ of $n$, there exists exactly one subgroup of $\langle a \rangle$ of order $d$, namely $\langle a^{n/d} \rangle$.

2. Sps $|a| = n$ and $H \leq \langle a \rangle$.

NTS: $|H| \mid n$.

from part 1, $H = \langle a^m \rangle$ where $m$ is the smallest positive integer such that $a^m \in H$. from our previous theorem,

$$|H| = |\langle a^m \rangle| = |a^m| = \frac{n}{\gcd(n,m)}$$

a divisor of n.

Thus $|H| \underbrace{\gcd(n,m)}_{\text{integer}} = n$

So, $|H| \mid n$. ✓

existence and uniqueness

**Thm** (Fundamental Theorem of Cyclic Groups) FTCG

Consider a cyclic group. Let $a$ be a generator of the group. (Thus the group can be expressed $\langle a \rangle$.)

1. Every subgroup of a cyclic group is cyclic.
2. If $\langle a \rangle$ has order $n$, the order of every subgroup of $\langle a \rangle$ is a divisor of $n$.
3. For each divisor $d$ of $n$, there exists exactly one subgroup of $\langle a \rangle$ of order $d$, namely $\langle a^{n/d} \rangle$.

3. Sps $|a| = n$ and suppose $d \mid n$, so $n = ds$ for some $s \in \mathbb{Z}$.

$s = \frac{n}{d}$ earlier thm

Then $|\langle a^s \rangle| = |a^s| = \frac{n}{\gcd(n,s)} = \frac{n}{s} = d.$

So $\langle a \rangle$ has a subgroup of order $d$. (existence)

Now, for uniqueness, sps $H \leq \langle a \rangle$ has order $d$. (NTS: $H = \langle a^{\frac{n}{d}} \rangle$)

We know $H = \langle a^m \rangle$ where $m$ is smallest positive integer such that $a^m \in H$. (want $m = \frac{n}{d}$)

Then, $m \mid n$ because if $n = mq + r$ with $0 \leq r < m$,

$e = a^n = a^{mq+r} = (a^m)^q a^r \Rightarrow a^r = (a^m)^{-q}$

which implies $a^r \in H$ (by closure) so $r = 0$. $\rightarrow$ so $n = mq$ ie. $m \mid n$.

Thus $n = mq$ so $\gcd(m,n) = m$. Therefore,

$$d = |H| = |\langle a^m \rangle| = |a^m| \overset{\text{previous thm}}{=} \frac{n}{\gcd(m,n)} = \frac{n}{m} \Rightarrow \boxed{m = \frac{n}{d}}$$

ie. $H = \langle a^m \rangle = \langle a^{n/d} \rangle$, as desired. ✓